PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor:	Jaroch et al.	Examiner:	Not yet assigned
Serial No.:	Filed herewith	Group Art Unit:	Not yet assigned
Filed:	Filed herewith	Docket No.:	04584.0021USC1
Title:	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS		

PRELIMINARY AMENDMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Dear Commissioner:

Prior to commencement of prosecution, please amend the above-identified application as follows:

Amendments to the Specification begin on page 2 of this paper.

Remarks/Arguments begin on page 3 of this paper.

Electronic Acknowledgement Receipt

EFS ID:	28405636
Application Number:	15437275
International Application Number:	
Confirmation Number:	4847
Title of Invention:	METHOD AND APPARATUS FOR PROVIDING ORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS
First Named Inventor/Applicant Name:	Joseph Jaroch
Customer Number:	23552
Filer:	Andrew T. Pouzeshi/Jacquelyn Slate
Filer Authorized By:	Andrew T. Pouzeshi
Attorney Docket Number:	04584.0021USC1
Receipt Date:	20-FEB-2017
Filing Date:	
Time Stamp:	17:13:52
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Application Data Sheet	2017-02-20-ADS-04584-0020USC1.PDF	1823709 86f403ca95ab71542fac95325a22caf5d611ea92	no	11

Warnings:

Information:					
2		2017-02-20-Application-04584-0021USC1.PDF	2413215 8bba73248cc2105ce9fc1c3b82a36d7b68018616	yes	45

Multipart Description/PDF files in .zip description		
Document Description	**Start**	**End**
Abstract	45	45
Claims	38	44
Specification	1	37

Warnings:					
Information:					
3	Drawings-only black and white line drawings	2017-02-20-Figures-04584-0021USC1.PDF	697076 12af69d4664cdb16bc0d0a11606f277049ec3b4a	no	15
Warnings:					
Information:					
4	Oath or Declaration filed	2017-02-20-Declaration-04584-0021USC1.PDF	822331 c0d8fcc33cd6b0b1482992f6f4147f27e231f4e7	no	8
Warnings:					
Information:					
5		2017-02-20-PrelimAmdt-04584-0021USC1.PDF	76263 c644c1447b49e1ad7dad422f72daef81163fa495	yes	3

Multipart Description/PDF files in .zip description		
Document Description	**Start**	**End**
Applicant Arguments/Remarks Made in an Amendment	3	3
Specification	2	2
Preliminary Amendment	1	1

Warnings:	
Information:	
Total Files Size (in bytes):	5832594

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	04584.0021USC1
	Application Number	
Title of Invention	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2:

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Joseph		Jaroch	

Residence Information (Select One) ● US Residency Non US Residency Active US Military Service

City	State/Province	Country of Residence
Deer Park	IL	US

Mailing Address of Inventor:

Address 1	c/o Webroot Inc.
Address 2	385 Interlocken Crescent, Suite 800

City	State/Province	Postal Code	Country
Broomfield	CO	80021	US

Inventor 2 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Jacques	Etienne	Erasmus	

Residence Information (Select One) ○ US Residency ● Non US Residency Active US Military Service

City	Country of Residence
Belper	GB

Mailing Address of Inventor:

Address 1	c/o Webroot Inc.
Address 2	385 Interlocken Crescent, Suite 800

City	State/Province	Postal Code	Country
Broomfield	CO	80021	US

Inventor 3 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Paul		Barnes	

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	04584.0021USC1
	Application Number	
Title of Invention	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS	

Residence Information (Select One) ○ US Residency ◉ Non US Residency Active US Military Service

City	Derby	Country of Residence [i]	GB

Mailing Address of Inventor:

Address 1	c/o Webroot Inc.		
Address 2	385 Interlocken Crescent, Suite 800		
City	Broomfield	State/Province	CO
Postal Code	80021	Country [i]	US

Inventor 4 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Johannes		Mayr	

Residence Information (Select One) ○ US Residency ◉ Non US Residency Active US Military Service

City	Linz	Country of Residence [i]	AT

Mailing Address of Inventor:

Address 1	c/o Webroot Inc.		
Address 2	385 Interlocken Crescent, Suite 800		
City	Broomfield	State/Province	CO
Postal Code	80021	Country [i]	US

Inventor 5 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Michael		Leidesdorff	

Residence Information (Select One) ◉ US Residency ○ Non US Residency Active US Military Service

City	Niwot	State/Province	CO	Country of Residence [i]	US

Mailing Address of Inventor:

Address 1	c/o Webroot Inc.		
Address 2	385 Interlocken Crescent, Suite 800		
City	Broomfield	State/Province	CO
Postal Code	80021	Country [i]	US

Inventor 6 Remove

Legal Name

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	04584.0021USC1
	Application Number	
Title of Invention	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS	

Prefix	Given Name	Middle Name	Family Name	Suffix
	Marco		Giuliani	

Residence Information (Select One) ○ US Residency ◉ Non US Residency Active US Military Service

City	Bastia Umbra	Country of Residence [i]	IT

Mailing Address of Inventor:

Address 1	c/o Webroot Inc.
Address 2	385 Interlocken Crescent, Suite 800

City	Broomfield	State/Province	CO
Postal Code	80021	Country [i]	US

Inventor 7 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Christopher	Jon	Williams	

Residence Information (Select One) ○ US Residency ◉ Non US Residency Active US Military Service

City	Derbyshire	Country of Residence [i]	GB

Mailing Address of Inventor:

Address 1	c/o Webroot Inc.
Address 2	385 Interlocken Crescent, Suite 800

City	Broomfield	State/Province	CO
Postal Code	80021	Country [i]	US

Inventor 8 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Chad	Edward	Bacher	

Residence Information (Select One) ◉ US Residency ○ Non US Residency Active US Military Service

City	Arvada	State/Province	CO	Country of Residence [i]	US

Mailing Address of Inventor:

Address 1	c/o Webroot Inc.
Address 2	385 Interlocken Crescent, Suite 800

City	Broomfield	State/Province	CO
Postal Code	80021	Country [i]	US

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	04584.0021USC1
	Application Number	
Title of Invention	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS	

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence Information of this application.**

Customer Number	23552		
Email Address	DOCKMPLS@merchantgould.com	Add Email	Remove Email

Application Information:

Title of the Invention	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS		
Attorney Docket Number	04584.0021USC1	**Small Entity Status Claimed**	☐
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	15	**Suggested Figure for Publication (if any)**	2

Filing By Reference:

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	04584.0021USC1
	Application Number	
Title of Invention	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS	

Please Select One:	● Customer Number	US Patent Practitioner	◯ Limited Recognition (37 CFR 11.9)
Customer Number	23552		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, 365(c), or 386(c) or indicate National Stage entry from a PCT application. Providing benefit claim information in the Application Data Sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.
When referring to the current application, please leave the "Application Number" field blank.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
	Continuation of	14/270069	2014-05-05
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
14/270069	Claims benefit of provisional	61/819470	2013-05-03

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button. Add

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55. When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX)[i] the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(i)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

Remove

Application Number	Country[i]	Filing Date (YYYY-MM-DD)	Access Code[i] (if applicable)

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button. Add

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	04584.0021USC1
	Application Number	
Title of Invention	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS	

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	04584.0021USC1
	Application Number	
Title of Invention	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS	

Authorization or Opt-Out of Authorization to Permit Access:

When this Application Data Sheet is properly signed and filed with the application, applicant has provided written authority to permit a participating foreign intellectual property (IP) office access to the instant application-as-filed (see paragraph A in subsection 1 below) and the European Patent Office (EPO) access to any search results from the instant application (see paragraph B in subsection 1 below).

Should applicant choose not to provide an authorization identified in subsection 1 below, applicant **must opt-out** of the authorization by checking the corresponding box A or B or both in subsection 2 below.

NOTE: This section of the Application Data Sheet is **ONLY** reviewed and processed with the **INITIAL** filing of an application. After the initial filing of an application, an Application Data Sheet cannot be used to provide or rescind authorization for access by a foreign IP office(s). Instead, Form PTO/SB/39 or PTO/SB/69 must be used as appropriate.

1. Authorization to Permit Access by a Foreign Intellectual Property Office(s)

A. Priority Document Exchange (PDX) - Unless box A in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the State Intellectual Property Office of the People's Republic of China (SIPO), the World Intellectual Property Organization (WIPO), and any other foreign intellectual property office participating with the USPTO in a bilateral or multilateral priority document exchange agreement in which a foreign application claiming priority to the instant patent application is filed, access to: (1) the instant patent application-as-filed and its related bibliographic data, (2) any foreign or domestic application to which priority or benefit is claimed by the instant application and its related bibliographic data, and (3) the date of filing of this Authorization. See 37 CFR 1.14(h)(1).

B. Search Results from U.S. Application to EPO - Unless box B in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the EPO access to the bibliographic data and search results from the instant patent application when a European patent application claiming priority to the instant patent application is filed. See 37 CFR 1.14(h)(2).

The applicant is reminded that the EPO's Rule 141(1) EPC (European Patent Convention) requires applicants to submit a copy of search results from the instant application without delay in a European patent application that claims priority to the instant application.

2. Opt-Out of Authorizations to Permit Access by a Foreign Intellectual Property Office(s)

☐ A. Applicant **DOES NOT** authorize the USPTO to permit a participating foreign IP office access to the instant application-as-filed. If this box is checked, the USPTO will not be providing a participating foreign IP office with any documents and information identified in subsection 1A above.

☐ B. Applicant **DOES NOT** authorize the USPTO to transmit to the EPO any search results from the instant patent application. If this box is checked, the USPTO will not be providing the EPO with search results from the instant application.

NOTE: Once the application has published or is otherwise publicly available, the USPTO may provide access to the application in accordance with 37 CFR 1.14.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	04584.0021USC1
	Application Number	
Title of Invention	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS	

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Applicant 1 — Remove

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

● Assignee	Legal Representative under 35 U.S.C. 117	Joint Inventor
Person to whom the inventor is obligated to assign.	Person who shows sufficient proprietary interest	

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor:

If the Applicant is an Organization check here. ☒

Organization Name	WEBROOT INC.		
Mailing Address Information For Applicant:			
Address 1	385 Interlocken Crescent		
Address 2	Suite 800		
City	Broomfield	**State/Province**	CO
Country	US	Postal Code	80021
Phone Number		Fax Number	
Email Address			

Additional Applicant Data may be generated within this form by selecting the Add button. Add

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	04584.0021USC1
	Application Number	
Title of Invention	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS	

Assignee 1

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication. An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

Remove

If the Assignee or Non-Applicant Assignee is an Organization check here. ☒

Organization Name	WEBROOT INC.

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1	385 Interlocken Crescent		
Address 2	Suite 800		
City	Broomfield	**State/Province**	CO
Country i	US	Postal Code	80021
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button. Add

Signature:

Remove

NOTE: This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b). **However, if this Application Data Sheet is submitted with the INITIAL filing of the application and either box A or B is not checked in subsection 2 of the "Authorization or Opt-Out of Authorization to Permit Access" section, then this form must also be signed in accordance with 37 CFR 1.14(c).**

This Application Data Sheet **must** be signed by a patent practitioner if one or more of the applicants is a **juristic entity** (e.g., corporation or association). If the applicant is two or more joint inventors, this form must be signed by a patent practitioner, **all** joint inventors who are the applicant, or one or more joint inventor-applicants who have been given power of attorney (e.g., see USPTO Form PTO/AIA/81) on behalf of **all** joint inventor-applicants.

See 37 CFR 1.4(d) for the manner of making signatures and certifications.

Signature	/Andrew T. Pouzeshi/			Date (YYYY-MM-DD)	2017-02-20
First Name	Andrew T.	Last Name	Pouzeshi	Registration Number	67672

Additional Signature may be generated within this form by selecting the Add button. Add

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	04584.0021USC1
	Application Number	
Title of Invention	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS	

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1 The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3 A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent CooperationTreaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ABSTRACT

Methods and systems for providing forensic visibility into systems and networks are provided. More particularly, a sensor agent may receive events defining an action of a first object acting on a target. The object, the event, and the target are then correlated to at least one originating object such that an audit trail for each individual event is created. A global perspective indicating an age, popularity, a determination as to whether the object may be malware, and IP/URL information associated with the event may then be applied to at least one of the object, the event, the target, and the originating object. A priority may then be determined and assigned to the event based on at least the global perspective. An event line containing event information is then transmitted to an end recipient where the information may be heuristically displayed.

What is claimed is:

1. A method comprising:

gathering one or more events defining an action of a first object acting on a target;

generating a contextual state for at least one of the one or more events by correlating the at least one event to an originating object, the contextual state including an indication of the originating object of the first object and an indication of at least one of a device on which the first object is executed and a user associated with the first object;

obtaining a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object, the information including at least one of age, popularity, a determination as to whether the first object is malware, a determination as to whether the originating object is malware; and Internet Protocol (IP) Address or Uniform Resource Locator (URL) information;

assembling an event line including details associated with the at least one event, the details including information uniquely identifying each of the first object, the action of the first object, the target, and the originating object; and

transmitting the assembled event line.

2. The method of claim 1, wherein the information associated with the one or more of the first object and the originating object is obtained from a community database; and

wherein the event line is transmitted to an end recipient.

3. The method of claim 1, further comprising:

obtaining an event priority based on one or more of the generated context and the global perspective for the at least one event, wherein the event line further includes the event priority for the at least one event.

4. The method of claim 1, wherein the at least one event includes information uniquely identifying the object performing the action, information uniquely

identifying the action being performed, and information uniquely identifying the target upon which the act is being performed.

5. The method of claim 4, further comprising:

determining whether a global perspective for the at least one event has been cached;

when the global perspective for the at least one event has been cached, obtaining a global perspective for the at least one event based on the cached global perspective; and

when the global perspective for the at least one event has not been cached, obtaining a global perspective for the at least one event from a community database.

6. The method of claim 5, further comprising:

determining whether the cached global perspective for the at least one event has expired; and

when the global perspective for the at least one event has expired, obtaining a global perspective for the at least one event from a community database.

7. The method of claim 4, further comprising:

heuristically displaying information identifying the first object performing the action, information identifying the action being performed, information identifying the target upon which the act is being performed, and the global perspective according to one or more of a location associated with the first object; at least one characteristic of an outbound connection associated with the first object; a dropped executable file; an age of the first object; and a number of concurrent connections associated with the first object.

8. A computer readable storage medium comprising processor executable instructions operable to perform the method of claim 1.

9. A system for providing forensic visibility into a system, comprising:

a device including:

a communication interface;

a processor;

data storage; and

a sensor agent stored on the data storage that is executable by the processor, wherein the sensor agent is operable to:

gather one or more events defining an action of a first object acting on a target;

generate a contextual state for at least one of the one or more events by correlating the at least one event to an originating object, the contextual state including an indication of the originating object of the first object and an indication of at least one of a device on which the first object is executed and a user associated with the first object;

obtain a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object, the information including at least one of age, popularity, a determination as to whether the first object is malware, a determination as to whether the originating object is malware; and Internet Protocol (IP) Address or Uniform Resource Locator (URL) information;

assemble an event line including details associated with the at least one event, the details including information uniquely identifying each of the first object, the action of the first object, the target, and the originating object; and

transmit the assembled event line utilizing the communication interface.

10. The system of claim 9, wherein the at least one of the one or more events is executed by the processor.

11. The system of claim 9, further comprising:

a global perspective information server; and

an end recipient device, wherein the information associated with the one or more of the first object and the originating object is obtained from the global perspective information server and the sensor agent transmits the event line to the end recipient.

12. The system of claim 8, wherein the sensor agent is further operable to:

cache the one or more events; and

asynchronously consolidate and normalize the one or more events.

13. The system of claim 9, wherein the at least one event includes information uniquely identifying the object performing the action, information uniquely identifying the action being performed, and information uniquely identifying the target upon which the act is being performed.

14. The system of claim 13, wherein the sensor agent is further operable to:

determine whether a global perspective for the at least one event has been cached;

when the global perspective for the at least one event has been cached, obtain a global perspective for the at least one event based on the cached global perspective; and

when the global perspective for the at least one event has not been cached, obtain a global perspective for the at least one event from a community database.

15. The system of claim 14, wherein the sensor agent is further operable to:

determine whether the cached global perspective for the at least one event has expired; and

when the global perspective for the at least one event has expired, obtain a global perspective for the at least one event from a community database.

16. The system of claim 13, wherein the end recipient heuristically displays information identifying the first object performing the action, information identifying the action being performed, information identifying the target upon which the act is being performed, and the global perspective according to one or more of a location associated with the first object; at least one characteristic of an outbound connection associated with

the first object; a dropped executable file; an age of the first object; and a number of concurrent connections associated with the first object.

17. A system for providing forensic visibility into a system, comprising:

a device including:

a communication interface;

a processor;

data storage; and

a sensor agent stored on the data storage that is executable by the processor, wherein the sensor agent is operable to:

gather one or more events defining an action of a first object acting on a target;

generate a contextual state for at least one of the one or more events by correlating the at least one event to an originating object, the contextual state including an indication of the originating object of the first object and an indication of at least one of a device on which the first object is executed and a user associated with the first object;

assemble an event line including details associated with the at least one event, the details including information uniquely identifying each of the first object, the action of the first object, the target, and the originating object; and

transmit the assembled event line utilizing the communication interface.

18. The system of claim 17, further comprising a global perspective information server including:

a processor;

a communication interface;

data storage; and

a global perspective module, wherein the global perspective module is operable to:

receive the event line from the device;

obtain a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object, the information including at least one of age, popularity, a determination as to whether the

first object is malware, a determination as to whether the originating object is malware; and Internet Protocol (IP) Address or Uniform Resource Locator (URL) information;

assemble a second event line including details associated with the at least one event, the details including information uniquely identifying each of the first object, the action of the first object, the target, and the originating object; and

transmit the assembled second event line utilizing the communication interface to an end recipient.

19. The system of claim 18, wherein the end recipient heuristically displays information identifying the first object performing the action, information identifying the action being performed, information identifying the target upon which the act is being performed, and the global perspective according to one or more of a location associated with the first object; at least one characteristic of an outbound connection associated with the first object; a dropped executable file; an age of the first object; and a number of concurrent connections associated with the first object.

20. The system of claim 17, further comprising a bridge including:

a processor;

a communication interface; and

a cached event store, wherein the cached event store is operable to:

receive a first request for a global perspective for the at least one event;

receive a second request for a global perspective for another event, the second request originating from another device;

obtain a first global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object, the information including at least one of age, popularity, a determination as to whether the first object is malware, a determination as to whether the originating object is malware; and Internet Protocol (IP) Address or Uniform Resource Locator (URL) information;

obtain a second global perspective for the another event;

provide the first global perspective to the device; and

provide the second global perspective to the another device.

METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS

CROSS-REFERENCE TO RELATED APPLICATIONS

This application claims the benefit of U.S. Provisional Patent Application Serial No. 61/819,470, filed May 3, 2013, the entire disclosure of which is hereby incorporated herein by reference.

FIELD

Methods and apparatuses for providing forensic visibility are described. More particularly, methods and systems for providing forensic visibility into client systems having full audit trails are described.

BACKGROUND

Network forensics generally relates to the capture, recording, and analysis of network events in order to discover the source of security attacks or other problem incidents. Network forensic systems generally utilize one of two approaches: the “catch it as you can approach” and the” stop, look, and listen approach.” “Catch it as you can” systems immediately write the packets to a disk file, buffering in memory as necessary, and perform analysis in batches. "Stop, look and listen" systems analyze the packets in memory, perform rudimentary data analysis and reduction, and write selected results to disk or to a database over the network.

However, existing network forensic tools, such as network sniffers and packet capturing tools, passively collect information about network traffic. Such tools may be able to detect and capture information associated with communication sessions, such as hostnames, ports, protocols, IP addresses, etc.; however, such tools tend to receive network events outside of a host or system. That is, a network forensic tool, such as a network sniffer, may reside at a network edge and may receive network events concerning the network from one or more hosts or systems. Accordingly, network edge devices have no ability to establish any sort of context from within the host or system that is generating the event. Therefore, devices residing at a network edge may monitor,

record, and or analyze network traffic between the host and the device, but information that may be useful within the host is not obtained.

For example, Figure 1 generally illustrates a comparative example including computing devices 104 and 108 in communication with a network edge device 116. The network edge device 116 may be commonly referred to as a "sniffer" which may monitor, capture, and analyze network traffic between the network edge device 116 and the computing devices 104 and 108. The network edge device 116 may further be in communication with a communication network 124, such as the internet. Accordingly, the network edge device 116 may monitor, capture, and analyze network traffic between the computing devices 104 and 108 and between the computing devices 104/108 and the communication network 124.

However, as previously mentioned, the network edge device 116 has no ability to monitor, capture, and/or analyze what is occurring within each of the computing device 104 and 108. In at least one comparative example, computing device 108 may contain or otherwise be infected with one or more pieces of malware. The term "malware" is used herein to refer generally to any executable computer file or, more generally "object", that is or contains malicious code, and thus includes viruses, Trojans, worms, spyware, adware, etc. and the like. Indeed, the network edge device 116 may be able to monitor, capture, and analyze communication traffic including the information, both encrypted and unencrypted, source and destination ports, source and destination IP address, and protocols utilized by the computing device 108, but the network edge device cannot provide details regarding files modified, registry entries changed, and/or new processes that are created. Accordingly, the network edge device 116 has no way of knowing to what extent the virus may have impacted the computing device 108, what additional files may have become infected, or what processes and/or objects operating are linked to the virus. What is needed therefore, is a solution that eliminates the guesswork and allows for end-to-end visibility of every event within a system and/or within a network.

SUMMARY

It is, therefore, one aspect of the present disclosure to provide a system and method whereby events occurring within a computing device are captured and additional

context and a global perspective is provided for each capture event. For example, a sensor agent may provide visibility into occurrences across an environment, such as a networked environment, to ensure that an administrator is aware of any system changes and data communication in and out of computing devices residing on the network. In this implementation, six components, or modules, may be utilized in the event gathering and processing: low level system filters, a local aggregator and interpreter, a context analyzer, a global perspective module, an event priority module, and an event distributor may be utilized to provide forensic visibility into one or more computing devices of a communication network.

The system filters may be built upon the same or similar technology related to behavior monitoring and collection, as discussed in U.S. Application Serial No. 13/372,375 filed February 13, 2012, "Methods and Apparatus for Dealing with Malware" (US-2012-0260340-A1), which is incorporated herein by reference in its entirety for all that it teaches and for all purposes. These filters intercept system events in a manner such that the operation of the system filter does not impact system performance, a key aspect of this solution. Events at this level tend to be very raw and generally not individually useful – on an average system, tens of millions of events take place every minute and the noise ratio can prevent forensic solutions from being able to provide sufficient value to the end consumer of their data due to the inability to quickly find important events. A product which impacts system performance will have considerably diminished value to an administrator and can negatively affect the results of an analysis undertaken. For example, a system filter that requires a majority of the available computing and system resources may render one or more communication devices unable to perform its primary function and may steer a real-time forensics analysis to an irrelevant analysis of events; irrelevant because such event analysis of information may be based on old and outdated event information. In some embodiments, events are gathered and timestamped accurately and sequentially, establishing a chronological order of system events for consumption at a higher level.

In at least one embodiment, the second component, the local aggregator and interpreter, receives events from the low level system filters, collecting them in batches from the queues in which they are inserted in real-time, and transmits these events to a

local service process where the events are held for further analysis. At this stage, intelligent caching may be invoked to drop events which are duplicates of recent events, and some data normalization may be performed to ensure consistency. Caching may be implemented sparingly but in critical areas to ensure redundant events are not continually reported – many applications perform thousands of the same events (network access to the same destination IP address, for example) and transmitting these events into an external log source would create a significant amount of unnecessary noise and potential performance degradation. The cache may integrate a "time to live" concept to prevent applications from hiding their traffic within their noise. The caches may automatically roll over to ensure sufficient space is always available without requiring exorbitant amounts of memory.

In addition, data normalization takes items such as kernel filenames, usermode filenames, process objects, registry objects, and other system structures and normalizes them into a standard format which is easy more easily consumed by automated parsers. Consolidating and normalizing data at this stage allows the data to be handled much more quickly at the higher levels to avoid reprocessing data and potentially missing events just because they were referred to slightly differently (\Device\HarddiskVolume1\Windows\file.exe instead of C:\Windows\file.exe for example). In some embodiments, an aspect of this subsystem provides the ability to process events asynchronously. The subsequent modules which will execute over the data can potentially take a considerable amount of time to complete but delaying the response for each event at this phase would result in a significant system slowdown. Instead, events are intelligently queued in multiple layers to minimize the number of individual threads but still ensure each event is given sufficient time to be independently processed. Because of this structure, there is no performance difference if an event takes one millisecond to be processed or one hour for the full series of routines to complete.

In at least some embodiments, the context analyzer is utilized to ensure that a user, such as a network administrator, is provided the deepest view of the most important data but still has access to the full range of data if they wish to see it. The analysis starts by correlating events to objects (their originating processes, devices, and users), and creating an audit trail for each individual event. This allows an administrator to

forensically track back any event which occurs to what triggered it. As previously discussed, conventional products in this space receive events outside of the system (for example, as a network edge device) and therefore have no ability to establish context within the system. The present solution eliminates the guesswork and allows for end-to-end visibility of every event from the bottom of the stack to the top. As contextual state is established, it is cached and aggregated to be quickly queried in subsequent lookups further reducing latency and improving the responsiveness of the system.

After the contextual analysis completes, the sensor agent attempts to establish a global perspective for each event by calling the cloud database using an infrastructure similar to the infrastructure discussed in U.S. Application Serial No. 13/372,375 filed February 13, 2012, "Methods and Apparatus for Dealing with Malware" (US-2012-0260340-A1), but with an additional layer capable of responding in a highly scalable manner which avoids the overhead generally associated with the complex rule processing within the overall database. This response includes information related to the age, popularity, and determination of an object – whether it is known good, bad, or unknown. This data may then be normalized and appended to each relevant portion of the event line. Further lookups are performed for network activity, assessing the reputation and category of each website and IP address as they are contacted.

The event priority module may contain priority logic, or one or more rule sets, to associate a priority to one or more events. The event priority module may utilize information from the local aggregator and interpreter, the context analysis module, and the global perspective module, to determine, or otherwise assign, a priority to an event; such a priority may be based on a rule set. The rule set may be provided by an administration system, backend system, end recipient 220, or other component of a forensic system.

The event distributor may then batch and transmit the events to the end recipient after the global perspective has been applied. In some embodiments, the event distributor may batch and transmit the events to the end recipient after the even priority has been determined. In one implementation, a syslog protocol may be used to send each event as a line of log data to be processed by an end consumer – usually a display/query engine. The transmission of events requires an additional layer of asynchronous processing as the

response time from the recipient cannot be allowed to slow down the higher level global perspective and contextual analysis work which is ongoing in other threads. Therefore, a transmission engine of the event distributor may build the final event line, packages it together with information about the host itself, and then send it directly into a separate queue where it will then be sent shortly after (usually a few seconds) while maintaining the pre-set timestamp of precisely when the event took place even if it is sent several seconds later.

The recipient of the event, whether hosted on a third party platform or using other proprietary software, may then display single events and/or perform wider analysis on groups of events, producing dashboard views and graphs to aid the administrator in identifying events that are most pertinent to their current investigation.

In accordance with at least one embodiment of the present disclosure, a method is provided, the method comprising gathering one or more events defining an action of a first object acting on a target; generating a contextual state for at least one of the one or more events by correlating the at least one event to an originating object, the contextual state including an indication of the originating object of the first object and an indication of at least one of a device on which the first object is executed and a user associated with the first object; obtaining a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object, the information including at least one of age, popularity, a determination as to whether the first object is malware, a determination as to whether the originating object is malware; and Internet Protocol (IP) Address or Uniform Resource Locator (URL) information; assembling an event line including details associated with the at least one event, the details including information uniquely identifying each of the first object, the action of the first object, the target, and the originating object; and transmitting the assembled event line.

In accordance with further embodiments of the present disclosure, a system is provided, the system comprising a device including a communication interface; a processor; data storage; and a sensor agent stored on the data storage that is executable by the processor, wherein the sensor agent is operable to: gather one or more events defining an action of a first object acting on a target; generate a contextual state for at least one of

the one or more events by correlating the at least one event to an originating object, the contextual state including an indication of the originating object of the first object and an indication of at least one of a device on which the first object is executed and a user associated with the first object; obtain a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object, the information including at least one of age, popularity, a determination as to whether the first object is malware, a determination as to whether the originating object is malware; and Internet Protocol (IP) Address or Uniform Resource Locator (URL) information; assemble an event line including details associated with the at least one event, the details including information uniquely identifying each of the first object, the action of the first object, the target, and the originating object; and transmit the assembled event line utilizing the communication interface.

In accordance with further embodiments of the present disclosure, a system is provided, the system comprising a device including a communication interface; a processor; data storage; and a sensor agent stored on the data storage that is executable by the processor, wherein the sensor agent is operable to: gather one or more events defining an action of a first object acting on a target; generate a contextual state for at least one of the one or more events by correlating the at least one event to an originating object, the contextual state including an indication of the originating object of the first object and an indication of at least one of a device on which the first object is executed and a user associated with the first object; assemble an event line including details associated with the at least one event, the details including information uniquely identifying each of the first object, the action of the first object, the target, and the originating object; and transmit the assembled event line utilizing the communication interface.

In accordance with at least one embodiment of the present disclosure, a method is provided, the method comprising obtaining an event line from one or more computing systems; parsing the event line to retrieve event information for at least one event, wherein the event information includes an event type, a contextual state for the event, a global perspective for the event, and a priority for the event; and displaying the event information for the at least one event to a display device.

In accordance with further embodiments of the present disclosure, a system is provided, the system comprising a device including a communication interface; a processor; data storage; a display device; and a parser stored on the data storage that is executable by the processor, wherein the parser is operable to: obtain an event line from one or more computing systems utilizing the communication interface; parse the event line to retrieve event information for at least one event, wherein the event information includes an event type, a contextual state for the event, a global perspective for the event, and a priority for the event; wherein the processor is operable to cause the event information for the at least one event to be displayed at a display device.

Additional features and advantages of embodiments of the present invention will become more readily apparent from the following description, particularly when taken together with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 illustrates a comparative example of a communication network, edge device, and one or more computing devices;

Figure 2 depicts a communication network including one or more computing systems, global perspective information server, and one or more end recipients in accordance with an exemplary embodiment of the present disclosure;

Figure 3 illustrates a block diagram depicting details of a computing system and a bridge in accordance with an exemplary embodiment of the present disclosure;

Figure 4 illustrates a block diagram depicting details of a global perspective information server and an end recipient in accordance with an exemplary embodiment of the present disclosure;

Figures 5A-C illustrates exemplary events, events having an applied contextual state, and events having an applied global perspective in accordance with an exemplary embodiment of the present disclosure;

Figure 6 illustrates a flow chart depicting details of at least one embodiment in accordance with an exemplary embodiment of the present disclosure;

Figure 7 illustrates a flow chart depicting operational details of a system filter in accordance with an exemplary embodiment of the present disclosure;

Figure 8 illustrates a flow chart depicting operational details of a local aggregator and interpreter in accordance with an exemplary embodiment of the present disclosure;

Figure 9 illustrates a flow chart depicting operational details of a context analyzer in accordance with an exemplary embodiment of the present disclosure;

Figure 10 illustrates a flow chart depicting operational details of a global perspective unit and/or global perspective module in accordance with an exemplary embodiment of the present disclosure;

Figure 11 illustrates a flow chart depicting operational details of an event priority generation unit in accordance with an exemplary embodiment of the present disclosure;

Figure 12 depicts a first data structure employed in accordance with at least some embodiments of the present disclosure; and

Figure 13 depicts one or more dashboards in accordance with at least some embodiments of the present disclosure.

DETAILED DESCRIPTION

Figure 1 depicts aspects of a system 200 for providing forensic visibility into one or more computing devices 204, 208, and 212 in accordance with at least one embodiment of the present disclosure. In general, the system 200 includes one or more computing device 204, each of which are interconnected to a global perspective information server 216 and end recipient 220 by one or more communication networks 212. The computing device 204 may comprise a general purpose computer, such as but not limited to a laptop or desktop personal computer 204B, a tablet computer, a smart phone 204A, or other device capable of communications over a communication network 212 and capable of presenting content to an associated user. The computing device 204 may also comprise a processing unit that is interconnected to an affiliated input/output device.

The communication network 212 may include one or more networks capable of supporting communications between nodes of the system 200, including but not limited to a computing devices 204A-C, the global perspective information server 216 and the end recipient 220. Examples of communication networks 212 include the Internet or any wide area network (WAN), local area network (LAN), or networks in various

combinations. Other examples of communication networks 212 in accordance with embodiments of the present disclosure include wireless networks, cable networks, satellite networks, and digital subscriber line (DSL) networks. In addition, different communication networks 212 may share a common physical infrastructure, for at least some portion of the physical network. For instance, a computing device 204 may be interconnected to a communication network 212 comprising the Internet and to a separate communication network between the computing device 204 and an end recipient 220.

The computing device 204 includes and/or executes a sensor agent 208 in connection with the presentation of content to the user. In accordance with at least one embodiment of the present disclosure, six components, or modules, may be utilized by the sensor agent 208 to gather and process events. The sensor agent 208 may include, but is not limited to, low level system filters, a local aggregator and interpreter, a context analyzer, a global perspective module, an event priority module, and an event distributor. Of course, and as can be appreciated by those skilled in the art, all six modules may not be required by the sensor agent 208. In at least one embodiment, the sensor agent may comprise fewer than six modules. That is, at least some functionality of the one or more modules may be provided by another device, such as a global perspective information server 216 for example. Moreover, it should be understood that the sensor agent 208 may include varying combination of modules. For example, the sensor agent 208 may include two of the six modules, three of the six modules, four of the six modules, or five of the six modules.

The system filters may intercept system events in a manner such that they do not impact system performance. Events may define those actions or behaviors of an object acting upon another object or some other entity. An object in this sense may be a computer file, part of a file or a sub-program, macro, web page or any other piece of code to be operated by or on the computer, or any other event whether executed, emulated, simulated or interpreted. Events may include, but are not limited to file activity, registry events, code events, network/internet events, process/thread events, window/GDI events, input events to name a few. An event may have three principal components: information and/or details describing the object performing the act (the "Actor"), information and/or details describing the act being performed (the "Event Type"), and information and/or

details describing the object or identity of another entity upon which the act is being performed (the "Victim" or “Target”). For example, the event data might capture the identity, e.g. the IP address or URL, of a network entity with which an object is communicating, another program acting on the object or being acted on by the object, a database or IP registry entry being written to by the object, etc. While simple, this structure allows a limitless series of behaviors and relationships to be defined. Examples of the three components of an event might include, but are not limited to, those illustrated in Table 1.

Table 1:

Actor	Event Type	Victim
Object 1	Creates Program	Object 2
Object 1	Sends data	IP Address 3
Object 1	Deletes Program	Object 4
Object 1	Executes	Object 2
Object 2	Creates registry key	Object 4

Moreover, in some embodiments, the Actor, Event Type, and/or Victim may be represented in the form of a so-called signature or key relating to the object key. Key generation is mainly to keep the data storage and transmission requirements as minimal as possible. The keys for each object may be formed by a hashing function operating on the object at the computing system 204. Accordingly, an event may include the three principal components as a key of the object performing the act (the "Actor"), a key of the act being performed (the "Event Type"), and the key of the object or identity of another entity upon which the act is being performed (the "Victim" or “Target”). Additionally, events at this level tend to be very raw and generally not individually useful – on an average system, tens of millions of events take place every minute and the noise ratio can prevent forensic solutions from being able to provide sufficient value to the end consumer of their data due to the inability to quickly find important events. Accordingly, in some embodiments, events are gathered and time stamped accurately and sequentially, establishing a chronological order of system events for consumption at a higher level.

The second component, the local aggregator and interpreter, receives events from the low level system filters in batches from the queues in which they are inserted in real-

time, and transmits them to the local service process where they are held for further analysis. In accordance with at least some embodiments of the present disclosure, the events may be cached and normalized such that kernel filenames, user mode filenames, process objects, registry objects, and other system structures are converted into a standard format for ease of consumption by one or more automated parsers. Following the aggregation and interpretation of the events, the context analyzer creates, or obtains, a contextual state by correlating events to objects and creating an audit trail for each individual event. In some instances, the sensor agent 208 of the computing device 204 may determine if contextual state information is available locally within a cache. If the contextual state information is not available locally, the sensor agent 208 of the computing device may obtain such contextual state information from a source of contextual state information accessible to the sensor agent 208.

Contextual state information may include, but is not limited to, originating processes, devices, and users. Additionally, contextual state information may include GenesisActor information and ancillary data. GenesisActor information may contain the object that is not the direct Actor of an event but which is the ultimate parent of the event being performed. For example in the case of a software installation, the GenesisActor would be the object that the user or system first executed and that initiated the software installation process, e.g. Setup.exe. Ancillary data may include data associated with the event type, actor and victim. For example, an event such as that used to record the creation of a registry run key may identify the Actor object as creating a registry run key, the event type itself (e.g. "regrunkey"), and the Victim or subject of the registry run key. The ancillary data in this case would define the run key entry itself; the Hive, Key name and Value. As a contextual state is established for each event, the contextual state may be cached and aggregated to be quickly queried in subsequent lookups further reducing latency and improving the responsiveness of the computing device 204. Contextual state information may be provided by the sensor agent 208 and/or a source of contextual state information accessible to the sensor agent 208. For example, the global perspective information server 216, in some embodiments, may be able to provide contextual state information to the sensor agent 208 for one or more events. Moreover, such contextual state information may be provided from one or more other computing devices 204.

After the contextual analysis completes, the sensor agent 208 establishes a global perspective for each event by calling on the global perspective information server 224. For example, the sensor agent 208 of the computing device 204 may determine if global perspective information is available locally within a cache. If the global perspective information is not available locally, the sensor agent 208 of the computing device 204 may issue a global perspective request 224 utilizing the communication network 212 and destined for the global perspective information server 216. The global perspective information server 216 may respond with global prospective information 228 and such information may be provided to the sensor agent 208 associated with the computing device 204.

The global perspective information 228 may include information related to the age, popularity, and determination of an object of the event – whether it is known good, bad, or unknown. The global perspective information may be retrieved or otherwise obtained for each object of an event and any objects provided as a part of a contextual information state. In some instances, the reputation and category of each website and IP address are obtained as they are contacted. Such information may then be normalized.

The event priority module may contain priority logic, or one or more rule sets, to associate a priority to one or more events. The event priority module may utilize information from the local aggregator and interpreter, the context analysis module, and the global perspective module, to determine, or otherwise assign, a priority to an event; such a priority may be based on a rule set. The rule set may be provided by an administration system, backend system, end recipient 220, or other component of a forensic system. For example, a rule set may determine that an event meeting certain conditions be assigned a priority according to a scale of severity. For instance, a rule set may specify that an event having a specific actor, victim, and/or origination process together with a global perspective indicating a specified age, popularity, malware determination, and/or IP/URL reputation be assigned an event priority representative of a potential risk assigned to the computing device 204 and/or network. Accordingly, when the event line containing event priority information is received at an end recipient 220, the end recipient 220 may be able to more easily identify events, and/or instances of malware, that require more immediate attention.

An event distributor of the sensor agent 208 may then create an event line comprising information from the event, information from the contextual state, information from the global perspective, and information from regarding the priority of the event. Alternatively, or in addition, an event distributor of the global perspective information server 216 may create an event line comprising information from the event, information from the contextual state, and information from the global perspective.

Accordingly, once the event distributor of the sensor agent 208 and/or the event distributor of the global perspective information server 216 create the event line for at least one event, the event line 244A-B may be sent to an end recipient 220 from the computing device 204 and/or the global perspective information server 216. The event distributor may batch and transmit the events to the end recipient 220 after the global perspective has been applied. In at least one implementation, the syslog protocol is utilized to send each event as a line of log data to be processed by an end consume such as a display/query engine like the product "splunk".

Alternatively, or in addition, some embodiments of the present disclosure may feature an optional bridge 222 which may be a dedicated device residing locally on a network. The bridge 222 may aggregate communications to and from one or more computing system 204 such that information to and from sensor agent 208 is cached at the bridge 222, optimizing global perspective requests and other communications. That is, the bridge may be shared across some or all devices in a network. In some embodiments, the bridge 222 may act as a local cache or data store for caching requests to the global perspective information server 216 and event lines directed to the end recipient 220. Additionally, the bridge 222 may perform selective or intelligent caching of global perspective information such that subsequent lookups or requests of global perspectives may be served from the local cache of the bridge 222.

Figure 3 illustrates additional aspects of a system 200 in accordance with embodiments of the present invention, and in particular illustrates additional features and components of a computing device 204 and a bridge 222. The computing device 204 may comprise a general purpose computer, tablet computer, smart phone, or other device or federated group of devices capable of supporting communications over a communication network 212. The computing device 204 may include a processor 316,

memory 304, one or more user input devices 308, such as a keyboard and a pointing device, and one or more user output devices 312, such as a display, speaker, and/or printer. Alternatively, or in addition, the user input 308 and the user output 312 may be combined into one device, such as a touch screen display. Computing device 204 may further include a communication interface 328 for communicating with another computing device 204, a global perspective information server 216, an end recipient 220, and/or the communication network 212.

Processor 316 is provided to execute instructions contained within memory 304 and/or storage 320. As such, the functionality of the computing device is typically stored in memory 304 and/or storage 320 in the form of instructions and carried out by the processor 304 executing such instructions. Accordingly, the processor 316 may be implemented as any suitable type of microprocessor or similar type of processing chip. One example of the processor 304 may include any general-purpose programmable processor, digital signal processor (DSP) or controller for executing application programming contained within memory 304 and/or storage 320. Alternatively, or in addition, the processor 316, memory 304, and/or storage 320, may be replaced or augmented with an application specific integrated circuit (ASIC), a programmable logic device (PLD), or a field programmable gate array (FPGA).

The memory 304 generally comprises software routines facilitating, in operation, pre-determined functionality of the computing device 204. The memory 304 may be implemented using various types of electronic memory generally including at least one array of non-volatile memory cells (e.g., Erasable Programmable Read Only Memory (EPROM) cells or FLASH memory cells, etc.). The memory 304 may also include at least one array of dynamic random access memory (DRAM) cells. The content of the DRAM cells may be pre-programmed and write-protected thereafter, whereas other portions of the memory may selectively be modified or erased. The memory 304 may be used for either permanent data storage and/or temporary data storage.

The data storage 320 may generally include storage for programs and data. For example, data storage 320 may provide storage for a sensor agent 208 including the system filters 340, the local aggregator and interpreter 344, the context analyzer 348, the global perspective module 352, the event distributor 356, and/or the general operating

system and other programs and data 324. Additionally, the data storage 320 may also include an event store 328, such as a database, for storing and/or caching event information, context information, global perspective information, and/or event lines. One or more components of the computing device 204 may communicate with one another utilizing a bus 336. Alternatively, or in addition, the sensor agent 208 may be provided separate and apart from data storage 320. That is, the sensor agent 208, including the system filters 340, the local aggregator and interpreter 344, the context analyzer 348, the global perspective module 352, the event priority generation unit 358, and the event distributor 356 may be implemented using a processor, such as a microprocessor 304. Accordingly, the microprocessor 304 may be specifically programmed to carry out one or more functions of the sensor agent 208. For example, the processor 304 may execute instructions associated with the sensor agent 208, including the system filters 340, the local aggregator and interpreter 344, the context analyzer 348, the global perspective module 352, the event priority generation unit 358, and the event distributor contained within memory 304 and/or storage 320. Alternatively, or in addition, the sensor agent 208, including the system filters 340, the local aggregator and interpreter 344, the context analyzer 348, the global perspective module 352, the event priority generation unit 358, and the event distributor 356 may share the processor 304.

The system filters 340 intercept system events in a manner such that they do not impact system performance. In some embodiments, events are gathered and time stamped accurately and sequentially such that a chronological order of system events is maintained and may be provided for consumption at a higher level. As one example, the time stamp may correspond to the time at which the event took place. Such a timestamp may be added to the event and/or maintained at an event line. Moreover, the system events may then be sorted according to event type and/or processing resources such that the system events are inserted, or stored, in a queue in real-time.

The local aggregator and interpreter receives events from the system filters 340, and collects the received events into batches from the queues in which they are inserted in real-time. The batches of events are then transmitted to a local service process where the events are held for further analysis. Such events may be held, or otherwise stored, within an event store 328. At this stage, intelligent caching may be invoked to drop

events which are duplicates of recent events, and some data normalization may be performed to ensure consistency. Caching may be implemented sparingly but in critical areas to ensure redundant events are not continually reported – many applications perform thousands of the same events (network access to the same destination IP address, for example) and transmitting these events into an external log source would create a significant amount of unnecessary noise and potential performance degradation. The cache may integrate a "time to live" concept to prevent applications from hiding their traffic within their noise. For example, events meeting predefined criteria may be dropped from the real-time system event queues. In some embodiments, if the predefined criteria include determining if a system event is the same or otherwise matches a previous system event, then the event may be dropped. Additionally, if a duplicate event occurs within a specified time, the event may be dropped from the queue. Alternatively, or in addition, if the duplicate system event occurs within a specified period of time, the duplicate system event may be modified to reflect that the duplicate system event is the same as a previously occurring system event. Accordingly, the later occurring duplicate system event may receive all contextual state information and global perspective information without requiring all of the determinations and/or lookups of such information. However, a time-to-live (TTL) functionality may be implemented on a cache basis to ensure that cached events, or previous events having context and/or a global perspective, are current. Accordingly, not all previous events having contextual information may be available to provide contextual information to a current event. As another option, the later occurring duplicate system event may be modified in a manner such that when the later occurring duplicate system event is interpreted by the end recipient 220, the end recipient 220 may determine that the system event information may be the same as a previously parsed system event line. Accordingly, a full event line for the duplicate system event is not generated and/or transmitted saving bandwidth and information processing resources. Further, the caches may automatically roll over to ensure sufficient space is always available without requiring exorbitant amounts of memory.

The local aggregator and interpreter 344 may additionally perform data normalization on items such as kernel filenames, user mode filenames, process objects,

registry objects, and other system structures and normalizes them into a standard format which is easy more easily consumed by automated parsers. Consolidating and normalizing data at this stage allows the data to be handled much more quickly at the higher levels to avoid reprocessing data and potentially missing events just because they were referred to slightly differently (\Device\HarddiskVolume1\Windows\file.exe instead of C:\Windows\file.exe for example). In some embodiments, an aspect of this subsystem provides the ability to process events asynchronously. The subsequent modules which will execute over the data may potentially take a considerable amount of time to complete but delaying the response for each event at this phase would result in a significant system slowdown. Instead, events are intelligently queued in multiple layers to minimize the number of individual threads but still ensure each event is given sufficient time to be independently processed. Because of this structure, there is little to no performance difference if an event takes one millisecond to be processed or one hour for the full series of routines to complete.

The context analyzer 348 ensures that a user at the end recipient 220 is provided with the deepest view of the most important data but still has access to the full range of data if they wish to see it. Accordingly, the context analyzer 348 correlates objects within system events to additional objects known to exist. For example, the context analyzer 348 may correlate an actor, victim, and/or event type to one or more originating processes, devices, and users. Such a correlation creates an audit trail for each individual event. As will be described later, this audit trail allows an administrator, at an end recipient 220 for example, to forensically track back any event which occurs to what triggered it. Accordingly, this additional information, including the originating processes, devices, and user, allows a contextual state to be established for each event. As each contextual state is established, the contextual state may be cached and aggregated to be quickly queried in subsequent lookups further reducing latency and improving the performance of the system.

After the context analyzer completes, the sensor agent 208 may attempt to establish a global perspective for each event by calling the cloud database utilizing an infrastructure similar to the infrastructure discussed in U.S. Application Serial No. 13/372,375 filed February 13, 2012, "Methods and Apparatus for Dealing with Malware"

(US-2012-0260340-A1, but with an additional layer capable of responding in a highly scalable manner which avoids the overhead generally associated with the complex rule processing within the overall database. Such an additional layer may be named SkyMD5. The response from the SkyMD5 layer may include information related to the age, popularity, and determination of an object – whether it is known good, bad, or unknown. This data may then be normalized and appended to each relevant portion of the event line. Further lookups are performed for network activity, assessing the reputation and category of each website and IP address as they are contacted.

In addition, similar to the contextual analyzer, the global perspective unit may first determine whether or not global perspective information for the particular system event is available locally. For example, global perspective information may be cached or otherwise stored in the storage data 320. In addition, a TTL approach may be additionally utilized to reduce the amount of traffic, or calls, to the global perspective information server 216, by the global perspective unit 352 of the sensor agent 208. Accordingly, contextual state information may only be available locally for a specified period of time and/or specified number of system events.

The event priority module 358 may contain priority logic, or one or more rule sets, to associate a priority to one or more events. The event priority module may utilize information from the local aggregator and interpreter 344, the context analysis module 348, and the global perspective module 352, to determine, or otherwise assign, a priority to an event; such a priority may be based on a rule set. The rule set may be provided by an administration system, backend system, end recipient 220, or other component of a forensic system. For example, a rule set may determine that an event meeting certain conditions be assigned a priority according to a scale of severity. Such an event priority may then be added to an existing event line or data structure.

The event distributor 356 may batch and transmit the events to the end recipient 220 after the global perspective has been applied. Alternatively, or in addition, the event distributor 356 may batch and transmit the events to the end recipient 220 after an event priority has been determined for the event. In one implementation, the syslog protocol is used to send each event as a line of log data to be processed by an end recipient 220. The transmission of events requires an additional layer of asynchronous processing as the

response time from the recipient cannot be allowed to slow down the higher level global perspective and contextual analysis work which is ongoing in other threads. Therefore, a transmission engine of the event distribute 356 builds the final event line, packages the event line together with information about the host itself, and then sends it directly into a separate queue where it will then be sent shortly after (usually a few seconds) while maintaining the pre-set timestamp of precisely when the event took place even if it is sent several seconds later. The separate queue may be a queue located in the storage data 320 and more specifically in the event store 328.

The bridge 222 may comprise a general purpose computer and/or server or other device or federated group of devices capable of supporting communications over a communication network 212. The bridge 222 may include a processor 382, memory 362, one or more user input devices 366, such as a keyboard and a pointing device, and one or more user output devices 378, such as a display, speaker, and/or printer. The bridge 222 may further include a communication interface 386 for communicating with another computing device 204, an end recipient 220, a global perspective information server 216, and/or the communication network 212. Processor 382 and memory 362 may be the same or similar as that which was described with respect to processor 316 and memory 304 respectively.

The data storage 370 may generally include storage for programs and data. For example, data storage 370 may provide storage for a cached event store 394 and/or the general operating system and other programs and data 374. Optionally, as indicated by the dashed line, the cached event store 394 may be separate and apart from the data storage 370. That is, the cached event store 394 functions independently and/or in cooperation with memory 362 and processor 382.

The bridge 222 may be a dedicated device residing locally on a network. The bridge 222 may aggregate communications to and from one or more computing system 204 such that information to and from sensor agent 208 is cached and stored at the cached event store 394, optimizing global perspective requests and other communications. Additionally, the bridge 222 may perform selective or intelligent caching of global perspective information such that subsequent lookups or requests of global perspectives

may be served from the cached event data store 394. One or more components of the bridge 222 may communicate with one another utilizing a bus 390.

Figure 4 illustrates additional aspects of a system 200 in accordance with embodiments of the present invention, and in particular illustrates additional features and components of a global perspective information server 216 and an end recipient 220. The global perspective information server 216 may comprise a general purpose computer and/or server or other device or federated group of devices capable of supporting communications over a communication network 212. The global perspective information server 216 may include a processor 464, memory 452, one or more user input devices 456, such as a keyboard and a pointing device, and one or more user output devices 460, such as a display, speaker, and/or printer. The global perspective information server 216 may further include a communication interface 468 for communicating with another computing device 204, an end recipient 220, and/or the communication network 212. Processor 464 and memory 452 may be the same or similar as that which was described with respect to processor 316 and memory 304 respectively.

The data storage 488 may generally include storage for programs and data. For example, data storage 488 may provide storage for a global perspective module 476, data store 486, and/or the general operating system and other programs and data 484. Optionally, each of the global perspective module 476, the data store 486, and/or the event distributor 492 may be separate and apart from the data storage 488. That is, as indicated by the dashed line, each of the global perspective module 476, the data store 486, and/or the event distributor 492 functions independently and/or in cooperation with memory 452 and processor 464.

The global perspective module 476 provides global perspective information at the request of a sensor agent 208. For example, and as previously described, the sensor agent 208 may transmit a global perspective request 224 to the global perspective information server 216 requesting global perspective information for one or more system events having a contextual state. Accordingly, the global perspective module 476 may provide the global prospective information 228 to the global perspective unit 352 of the computing system 204. In addition, in some embodiments the event distributor functionality may reside at the global perspective information server 216. Accordingly,

in such an embodiment, the global perspective module 476 may receive event information having contextual state information. In such an instance, the global perspective module 476 may provide the global perspective information and store the system event, contextual information, and global perspective information in data store 486. The event distributor 492 may then assemble the event line information, queue the event line for transmission, and transmit the event line to the end recipient 220. The event distributor 492 may function and/or operate in a manner similar to or the same as the event distributor 356 of the sensor agent 208. One or more components of the global perspective information server 216 may communicate with one another utilizing a bus 472.

The end recipient 220 may comprise a general purpose computer and/or server or other device or federated group of devices capable of supporting communications over a communication network 212. The end recipient 220 may include a processor 416, memory 404, one or more user input devices 408, such as a keyboard and a pointing device, and one or more user output devices 412, such as a display, speaker, and/or printer. The end recipient 220 may further include a communication interface 428 for communicating with another computing device 204, a global perspective information server 216, and/or the communication network 212. Processor 416 and memory 404 may be the same or similar as that which was described with respect to processor 316 and memory 304 respectively.

The end recipient 220 may further include data storage 420 which may include storage for programs and data. For example, data storage 420 may provide storage for an event line parser 440, a user interface generator 444, a global information store 448, and/or the general operating system and other programs and data 420. Optionally, as indicated by the dashed line, each of the event line parser 440, the user interface generator 444, and the global information store 448 may be provided separate and apart from the data storage 436 where each of the event line parser 440, a user interface generator 444, and the global information store 448 functions independently and/or in cooperation with memory 404 and processor 416. One or more components of the end recipient 220 may communicate with one another utilizing a bus 432.

The event line parser 440 may parse an incoming event line 244A-B and store the event lines, either parsed or whole, at the global information store 448. Accordingly, the end recipient 220 may utilize the parsed event line to generate an user interface utilizing the user interface generator 444. The generated user interface may then be displayed to a user at an user output device 412. The user interface generator 444 may create one or more dashboards that provide information to a user of the end recipient 220. Accordingly, dashboards may display correlated events collected by a sensor agent 204. Such correlated events may comprise File System/Disk activity, network activity, and registry activity on the endpoint along with the global community data and IP and domain reputation data to provide a complete point of view of the computing system 204 activity and further provide a full meaning to every single reported event. Accordingly, spotting and highlighting behaviours in the event data from computing systems 204 may potentially assist in finding and determining whether such activity is malicious or not.

Moreover, there may exist multiple dashboards each of which provide a specific heuristic that targets a specific potential malicious behaviour. For example, a first dashboard generally looks for executables that have been found and executed from specific critical paths in the computing system 204; those paths that are known to host malware executables (browser's cache, temporary files folder, system32 folder, auto start folder and so on). The dashboard may filter those files determined as good, unknown and bad from global community information. For unknown files, the dashboard may show their popularity at the global community, i.e. on how many computing systems 204 they have been seen - and if they establish outbound internet connections. If such files connect to the Internet, the dashboard may trace down and identify the specific connection and geo-locate the destination address on a world map.

In another embodiment, a separate dashboard may analyze outbound connections from the analyzed endpoints. Accordingly, this dashboard may filter out and highlight connections to high-risk countries, i.e. those countries known to host malicious servers, and retrieve software that actually established the suspicious connections. The dashboard may also provide another point of view; that is, the dashboard may highlight all connections to specific IPs and domains that have been set up recently (e.g. in the last 60 days). All connections may be shown on a map view and the contacted IPs and domains

are crosschecked with a database to determine their reputation and website category (if known).

As another example, a dashboard may highlight potential exploits detected on the endpoint by monitoring the most common software usually installed on an average computing system 204 and targeted by exploit attacks. The dashboard may generally identify software like Java, Adobe Acrobat, Microsoft Office, Flash Player and monitor if such software is dropping executable files on the system. Accordingly, if the software behaves in this manner, such a behaviour should be considered a suspicious behaviour, as software should not be dropping any executable files on the system. If such an occurrence is detected, the dashboard may analyze the dropped executable for its popularity in the global community and then identify potential outbound connections established by the just-dropped executable. If an outbound connection is found, the dashboard retrieves the destination IP and renders, or draws, the location of the IP address on a map view, such as a world map.

As another example, a separate dashboard may highlight those new processes created on the monitored computing systems 204 that are undetermined and have only been recently seen in the global community. For every process, a lifetime scheme is assembled which allows the administrator to understand when the undetermined file firstly landed on the endpoint and for how long time it has been active on the system. This dashboard may further provide specific events triggered by the suspicious process while active on the system.

As another example, a dashboard may highlight system processes that have been found to establish concurrent connections to different IPs in less than a specific timeframe and/or threshold, such as one second. If found, the system processes may be suspect and deemed to host malicious code; such malicious code having been injected into the website. For every established connection, the dashboard may trace and identify the contacted country and the specific IP/domain. As another example, a dashboard may be generated by the user interface generator 448 such the dashboard monitors activities on remote storage services like Dropbox, showing the filename and size of the files being saved on a remote server. The dashboard may further monitor and identify sensitive or

classified company data that may be in the process of being stolen or placed (i.e. saved, stored, etc.) on a non-approved storage location.

Figures 5A-5C illustrate additional aspects of a system 200 in accordance with embodiments of the present invention, and in particular illustrates event capturing, the application of contextual state, and the application of a global perspective to such captured events. For example, events 508A-520A are representative events that may have been captured by one or more system filters 340 of a sensor agent 204. The system events 504A-520A may include an Event ID, an Event Type, an Actor and a Victim. Although not illustrated, a timestamp may also be included in the event. As previously described, the actor and the victim may comprise objects. For example, in the system event 520A, an event type of Registry Edit is captured where Object 2 is modifying Object 3; accordingly, Object 3 may be the registry hive, a specific registry entry, and/or a specified registry value. Moreover each of the Event ID, Event Type, Actor, and Victim may be hashed resulting in a key that uniquely identifies the data.

As illustrated in Figure 5B, a contextual analysis may be applied to the captured events 504B-520B. Accordingly, a context 520B comprising an origination proceess, Device, User, and in some instances, a GenesisActor may further supplement or enhance the Event ID, Event Type, Actor, and Victim. Although illustrated as including an originating process, GenesisActor, device, and user, the contextual information forming the contextual state 520B may include more or less information and in varying combinations. Moreover, as illustrated in Figure 5B, the originating process or object may determined based on a previous event that initiated or otherwise created the current process and/or object. Additionally, as illustrated in Figure 5B, the GenesisActor is determined based on a chain of previous events. For example, the Actor of Object 1 for system event 504B of Event Type "executes" operates on Filename 1. Object 1 subsequently creates a process Object 2 in 508B which is further utilized in both 516B and 520B. Accordingly, as the Object 1 initiated subsequent events, Object 1 may be determined to be the GenesisActor for 520B, 516B, 512B, and 508B.

As illustrated in Figure 5C, a global perspective is applied to event 520C. The global perspective may comprise information for each object in the event and/or the contextual state 524. For example, a global perspective may be obtained for Object 2,

Object 3, and Object 1 as illustrated. Accordingly, a global perspective 528 indicating the age of Object 2, the popularity of Object 2, the determination of Object 2, and/or additional IP/URL information of Object 2 may be provided. Similar global perspective information 532, 536 may be obtained for Object 3 and Object 1 respectfully. Accordingly, an event line may be assembled utilizing the event information, contextual state, and global perspective information. In addition, the global perspective may provide additional information pertaining to an IP/URL address. For example, such information may include a categoryID of the IP/URL, a confidence of such a categoryID, a reputation, geolocation information such as which country the IP/URL is associated with, and/or a threat history associated with the IP/URL.

Referring now to Figure 6, a method 600 for providing forensic visibility into a system is provided in accordance with embodiments of the present disclosure. Method 600 is in embodiments, performed by a device, such as the sensor agent 204 and/or the end recipient 220. More specifically, one or more hardware and software components may be involved in performing method 600. In one embodiment, one or more of the previously described units perform one or more of the steps of method 600. The method 600 may be executed as a set of computer-executable instructions executed by a computer system and encoded or stored on a computer-readable medium. Hereinafter, the method 600 shall be explained with reference to systems, components, units, software, etc. described with Figures 1-5C.

Method 600 may continuously flow in a loop, flow according to a timed event, or flow according to a change in an operating or status parameter. Method 600 is initiated at step 604 where events of a computing system 204 may be initiated. At step 608, such an event may be detected. As previously discussed, the events, which may comprise system events, may be detected by one or more system filters 340 of a sensor agent 208. The sensor agent 208 may be comparatively small compared with other commercially available forensic tools and anti-malware software. This may be achieved by the sensor agent 204 being developed in a low-level language, having direct access to system resources such as the video display, disk, memory, the network(s), and without the incorporation of many standard code or dynamic linked libraries to perform these functions. Memory usage may be optimized by storing data in a local database structure

that provides the ability to refer to objects by a unique identifier rather than requiring full filenames or signatures. All unnecessary dynamic link libraries are unloaded from the process immediately as they are identified as no longer being used, and background threads are merged to reduce CPU usage. A small, efficient sensor agent 204 may be deployed more quickly and may be used alongside other programs, including other security programs, with less load on or impact on the computer's performance. This approach also has the advantage of having less surface area for attack by malware making it inherently more secure.

Method 600 then proceeds to step 612 where the local aggregator and interpreter 344 receives events from the low level system filters 340, collecting them in batches from the queues in which they are inserted in real-time. As previously discussed, intelligent caching may be invoked to drop events which are duplicates of recent events. Further, some data normalization may be performed at step 612 to ensure consistency. Further still, caching may be implemented sparingly but in critical areas to ensure redundant events are not continually reported. Method 600 then proceeds to step 616 where a contextual state may be applied by a context analyzer 348 to the event information. Accordingly, the context analyzer correlates events to objects such that an audit trail for each individual event is created. As a contextual state is established, it is cached and aggregated to be quickly queried in subsequent lookups further reducing latency and improving the responsiveness of the system. Once a contextual state is applied, method 600 then proceeds to step 620 where a global perspective is applied for each event and/or each object of the event and contextual state. Accordingly, information related to the age, popularity, and determination of an object – whether it is known good, bad, or unknown is obtained. In addition, as previously mentioned, the global perspective may contain information pertaining specifically to an IP/URL address. For example, the global perspective may include information relating network activity and an assessment of the reputation and category of each website and IP address as they are contacted. This data may then be normalized. Method 600 then proceeds to step 622 where an event priority may be applied to the event. As previously discussed, the event priority may be obtained utilizing a rule set and applying such a rule set to aggregated event information, contextual state information, and global perspective information. Accordingly, method

600 then proceeds to step 624 where such data is appended to each relevant portion of an event line.

Method 600 may then proceed to step 628 where the event distributor 356 may transmit the event line 244 to the end recipient 220. The event distributor may first assemble the information and transmit the batched information after the global perspective has been applied. Once at the end recipient, the method 600 may then parse the event line at step 632 to filter out one or more events. Accordingly, the events may be stored in the data store 480. Method 600 may then display the parsed event line at one or more dashboards in accordance with step 636. Method 600 then ends at step 640.

Referring now to Figure 7, additional details regarding step 608 of method 600 is provided in method 700. Method 700 is in embodiments, performed by a device, such as the sensor agent 204 and/or the system filter 340. More specifically, one or more hardware and software components may be involved in performing method 700. In one embodiment, one or more of the previously described units perform one or more of the steps of method 700. The method 700 may be executed as a set of computer-executable instructions executed by a computer system and encoded or stored on a computer-readable medium. Hereinafter, the method 700 shall be explained with reference to systems, components, units, software, etc. described with Figures 1-6.

Method 700 may continuously flow in a loop, flow according to a timed event, or flow according to a change in an operating or status parameter. Method 700 is initiated at step 704 where events of a computing system 204 may be initiated. At step 708, such an event may be detected. As previously discussed, the events, which may comprise system events, may be detected by one or more system filters 340 of a sensor agent 208. Accordingly, at step 712, an event record may be created. The event record may be the same or similar to that which was described with respect to Figure 5A. Accordingly, the event record may include an Event ID, and Event Type, an Actor, and a Victim. Moreover, in some embodiments, instead of creating a separate event record and a separate event line, a single event line for each event may be utilized. That is, the event record may be the event line. Accordingly, at step 716 the event line and/or the event record may be time stamped and stored. At step 720, method 700 may then determine which queue the event record or event line, should be assigned. In some embodiments,

the event record/event line may be assigned to a specified queue based on the event type. Alternatively, or in addition, the event record/event line may be assigned to a specified queue based on the needed resources and the available resources. Method 700 then ends at step 724.

Referring now to Figure 8, additional details regarding step 612 of method 600 is provided in method 800. Method 800 is in embodiments, performed by a device, such as the sensor agent 204 and/or the local aggregator and interpreter 344. More specifically, one or more hardware and software components may be involved in performing method 800. In one embodiment, one or more of the previously described units perform one or more of the steps of method 800. The method 800 may be executed as a set of computer-executable instructions executed by a computer system and encoded or stored on a computer-readable medium. Hereinafter, the method 800 shall be explained with reference to systems, components, units, software, etc. described with Figures 1-7.

Method 800 may continuously flow in a loop, flow according to a timed event, or flow according to a change in an operating or status parameter. Method 800 is initiated at step 804. Method 800 then proceeds to step 808 where batches of event records/event lines are received form one or more previously described queues. For each event, method 800 proceeds to determine if the event record/event line meets a predefined criteria. For example, if the current event record/event line matches or is otherwise the same as a previous event record/event line, method 800 may proceed to step 824 where the current event record/event line may be dropped. Alternatively, or in addition, the dropped event record/event line may be modified such that either the contextual analyzer 348 and/or the global perspective unit 352 may be able to determine a contextual state and global perspective based on a previously captured event record/event line. Alternatively, or in addition, the dropped event record/event line may be modified to refer to a previously captured event record/event line such that upon parsing by the end recipient 220, the current event line/event record is provided meaning from a previously parsed event record/event line

Accordingly, method 800 may then proceed to step 816 where the information may be normalized. The normalization may be implemented with a database which takes complete path names and translates them to representatives paths. So, for example, the

Windows\file.exe would end up normalized to %windir%\file.exe, allowing rules to be created for any full path. Similar logic is utilized for paths like %appdata% which would have unique elements per-user and would be difficult to manage if not normalized. Accordingly, once the information in the event record/event line is normalized, method 800 may proceed to step 820 where the events may be intelligently queued. For instance, each event record/event line may be placed in a queue according to an event type. Method 800 may then end at step 828.

Referring now to Figure 9, additional details regarding step 616 of method 600 is provided in method 900. Method 900 is in embodiments, performed by a device, such as the sensor agent 204 and/or the context analyzer 348. More specifically, one or more hardware and software components may be involved in performing method 900. In one embodiment, one or more of the previously described units perform one or more of the steps of method 900. The method 900 may be executed as a set of computer-executable instructions executed by a computer system and encoded or stored on a computer-readable medium. Hereinafter, the method 900 shall be explained with reference to systems, components, units, software, etc. described with Figures 1-8.

Method 900 may continuously flow in a loop, flow according to a timed event, or flow according to a change in an operating or status parameter. Method 900 is initiated at step 904. Method 900 then proceeds to step 908 where event records/event lines are received. Method 900 then proceeds to step 912 where objects of the event record/event line are correlated to objects in a contextual state. For example, and as illustrated in at least Figure 5B, a contextual state may include originating processes, devices, and users. Accordingly, once objects of the event record/event line have been correlated, method 900 proceeds to step 916 where the event record/event line includes an established contextual state. In some embodiments consistent with the present disclosure, the contextual state may already be cached and may be obtained based on the event record/event line information. As one example, based on the event type, actor, and victim, it may be possible to recover a contextual state that includes an originating process, the device, and the user. However, not all cached instances of cached contextual state will suffice as different users may utilize a computing device 204.

Method 900 then proceeds to step 920 where the contextual state may be cached and made accessible for later access. In accordance with at least one embodiment, the event line may be partially assembled where the partially assembled event line may include various combinations of the event type, the actor object, the victim object, and the origination process. Accordingly, the partially assembled event line may later be passed to a global perspective information server. As such, method 900 ends at step 928.

Referring now to Figure 10, additional details regarding step 620 of method 600 is provided in method 1000. Method 1000 is in embodiments, performed by a device, such as the sensor agent 204 and/or the global perspective unit 352, the global perspective module 476, and/or the global perspective information server 216. More specifically, one or more hardware and software components may be involved in performing method 1000. In one embodiment, one or more of the previously described units perform one or more of the steps of method 1000. The method 1000 may be executed as a set of computer-executable instructions executed by a computer system and encoded or stored on a computer-readable medium. Hereinafter, the method 1000 shall be explained with reference to systems, components, units, software, etc. described with Figures 1-9.

Method 1000 may continuously flow in a loop, flow according to a timed event, or flow according to a change in an operating or status parameter. Method 1000 is initiated at step 1004. Method 1000 then proceeds to step 1008 where method 1000 determines whether event record/event line information is cached. Such a determination may be based upon whether the event information, such as the event type, the actor, and/or the victim, match a predetermined criteria. For instance, not all event types may be cached. In one embodiment, global perspective information caching will cache a specific number of event types occurring within a specified time period. In other instances, all global perspective information for all events may be cached. Accordingly, if it is determined that global perspective information is not cached, method 1000 proceeds to step 1016 where the global perspective information server may be contacted. Accordingly, such a request may provide the global perspective information server 216 with information in an event record and/or a partially assembled event line. Accordingly, the global perspective information or a particular event may be retrieved. The retrieved

global perspective information may then be stored at step 1024. For example, such information may be stored in event store 328.

Otherwise, if global perspective information is cached for an event record/event line, the method 1000 may proceed to step 1012 were method 1000 may determine whether a time-to-live (TTL) has been exceeded. In some instances, the cached information may expire based on the frequency of occurrence for a particular event. For example, if an event occurs with a high frequency, the global perspective unit 352 may determine that for efficiency reasons, either resources and/or bandwidth, caching for a particular event would be beneficial to improving the overall efficiency of the sensor agent 208 and/or computing device 204. Accordingly, the method 1000 then proceeds to step 1020 where the global perspective for the event is retrieved based on the cached entry. Otherwise, if the occurrence of the same event happens at a reduced frequency such that it would not be beneficial to cache global perspective information, it might be more beneficial to directly lookup and retrieve such information directly from the global perspective information server 216. Accordingly, the method 1000 proceeds to step 1016 where global perspective information is received from the global perspective information server. In some instances, the cache of global perspective events may expire according to a predetermined time. At step 1024, method 1000 may proceeds to step 1028 where method 1000 ends.

Referring now to Figure 11, additional details regarding step 624 of method 600 is provided in method 1100. Method 1100 is in embodiments, performed by a device, such as the sensor agent 204. More specifically, one or more hardware and software components may be involved in performing method 1100. In one embodiment, one or more of the previously described units perform one or more of the steps of method 1100. The method 1100 may be executed as a set of computer-executable instructions executed by a computer system and encoded or stored on a computer-readable medium. Hereinafter, the method 1100 shall be explained with reference to systems, components, units, software, etc. described with Figures 1-10.

Method 1100 may continuously flow in a loop, flow according to a timed event, or flow according to a change in an operating or status parameter. Method 1100 is initiated at step 1104. Method 1100 then proceeds to step 1108 where a priority rule set

is retrieved. The priority rule set may be retrieved directly from an administration system and/or may be received locally from a storage location associated with the sensor agent 208 and/or the data storage 320. The priority rule set may have one or more predefined criteria for assigning a priority level to an event. The priority level may represent a perceived severity or risk in which such an event poses. Method 1100 then proceeds to step 1112 where an event priority, or level, is assigned to the event.

In at least one embodiment, the priority level may be derived from aggregated and interpreted event information from the local aggregator and interpreter 344, context analyzer 348, and global perspective unit 352. Accordingly, an event having a specified Actor, Victim, Target, originating process, or the like together with a global perspective indicating that at least one of the Actor, Victim, Target, origination process has been determined to be malware may result in a rule set that assigns a priority level to the event indicating that such the event should be immediately brought to the attention of an administrator. Accordingly, the event may be said to have a "high" priority or be a "high" priority event. Method 1100 may then end at step 1116.With reference to Figure 12, details of a data structure 1200 will be described in accordance with embodiments of the present disclosure. In some embodiments, the data structure 1200 may be used as an event line and may contain details specific to an event, context, and global perspective. For example, an event line 1204 may generally include, without limitation, event information 1208, a time stamp 1212, context state information 126, global perspective information 1220, and a priority level 1222, where the priority may be a value that ranges between a low and a high number. In some embodiments, the event field 1208 may further include Event ID information 1224, Event Type information 1228, Actor 1232, and Victim information 1236. In some embodiments, the context state 1216 may include, without limitation, Originating Process 1240 information, Device information 1244, User information 1248, dependent data such as, but not limited to additional meta data and/or ancillary data describing or containing detailed information about one or more objects 1252, and object info 1256. In addition, the global perspective field may include, but is not limited to an age 1260, popularity 1264, malware determination 1268, and/or IP/URL information 1272, where IP/URL information may include, but is not limited to a categoryID of the IP/URL, a confidence of such a categoryID, a reputation, geolocation

information such as which country the IP/URL is associated with, and/or a threat history associated with the IP/URL. Of course, additional relevant information may be included in the event line 1204 depending on the event.

Figure 13 generally illustrates exemplary user interfaces, or dashboards 1304, 1332, and 1336, which may be displayed at an end recipient 220 to a user at an user output device 412. The user interface generator 444 may create the one or more dashboards 1304, 1332, and 1336 to provide information from an event to a user of the end recipient 220. Accordingly, the dashboards 1304, 1332, and 1336 may display correlated events collected by a sensor agent 204. Such correlated events may comprise File System/Disk activity 1308, network activity 1312, and registry activity 1316 on the endpoint along with the global community data and IP and domain reputation data 1324 to provide a complete point of view of the computing system 204 activity and further provide a full meaning to every single reported event, including at least one of an originating process, an Event Type, a Target, a Victim, and a Actor. Accordingly, spotting and highlighting behaviours in the event data from computing systems 204 may potentially assist in finding and determining whether such activity is malicious or not.

Moreover, there may exist multiple dashboards 1304, 1332, and 1336 each of which provide a specific heuristic that targets a specific potential malicious behaviour. For example, a first dashboard 1326 generally looks for executables that have been found and executed from specific critical paths in the computing system 204; those paths that are known to host malware executables (browser's cache, temporary files folder, system32 folder, auto start folder and so on). The dashboard 1326 may filter those files determined as good, unknown and bad from global community information. For unknown files, the dashboard may show their popularity at the global community, i.e. on how many computing systems 204 they have been seen - and if they establish outbound internet connections. If such files connect to the Internet, the dashboard 1332 may trace down and identify the specific connection and geo-locate the destination address on a world map.

In another embodiment, a separate dashboard 1336 may analyze outbound connections from the analyzed endpoints. Accordingly, this dashboard may filter out and highlight connections to high-risk countries, i.e. those countries known to host malicious

servers, and retrieve software that actually established the suspicious connections. The dashboard 1336 may also provide another point of view; that is, the dashboard 1336 may highlight all connections to specific IPs and domains that have been set up recently (e.g. in the last 60 days). All connections may be shown on a map view and the contacted IPs and domains are crosschecked with a database to determine their reputation and website category (if known).

As another example, a dashboard 1340 may highlight potential exploits detected on the endpoint by monitoring the most common software usually installed on an average computing system 204 and targeted by exploit attacks. The dashboard 1340 may generally identify software like Java, Adobe Acrobat, Microsoft Office, Flash Player and monitor if such software is dropping executable files on the system. Accordingly, if the software behaves in this manner, such a behaviour should be considered a suspicious behaviour, as software should not be dropping any executable files on the system. If such an occurrence is detected, the dashboard 1340 may analyze the dropped executable for its popularity in the global community and then identify potential outbound connections established by the just-dropped executable. If an outbound connection is found, the dashboard 1340 retrieves the destination IP and renders, or draws, the location of the IP address on a map view, such as a world map.

As another example, a separate dashboard 1344 may highlight those new processes created on the monitored computing systems 204 that are undetermined and have only been recently seen in the global community. For every process, a lifetime scheme is assembled which allows the administrator to understand when the undetermined file firstly landed on the endpoint and for how long time it has been active on the system. This dashboard 1344 may further provide specific events triggered by the suspicious process while active on the system.

As another example, a dashboard 1348 may highlight system processes that have been found to establish concurrent connections to different IPs in less than a specific timeframe and/or threshold, such as one second. If found, the system processes may be suspect and deemed to host malicious code; such malicious code having been injected into the website. For every established connection, the dashboard may trace and identify the contacted country and the specific IP/domain. As another example, a dashboard 1348

may be generated by the user interface generator 448 such the dashboard monitors activities on remote storage services like Dropbox, showing the filename and size of the files being saved on a remote server. The dashboard 1348 may further monitor and identify sensitive or classified company data that may be in the process of being stolen or placed (i.e. saved, stored, etc.) on a non-approved storage location.

In the foregoing description, for the purposes of illustration, methods were described in a particular order. It should be appreciated that in alternate embodiments, the methods may be performed in a different order than that described. It should also be appreciated that the methods described above may be performed by hardware components or may be embodied in sequences of machine-executable instructions, which may be used to cause a machine, such as a general-purpose or special-purpose processor or logic circuits programmed with the instructions to perform the methods. These machine-executable instructions may be stored on one or more machine readable mediums, such as CD-ROMs or other type of optical disks, floppy diskettes, ROMs, RAMs, EPROMs, EEPROMs, magnetic or optical cards, flash memory, or other types of machine-readable mediums suitable for storing electronic instructions. Alternatively, the methods may be performed by a combination of hardware and software.

Furthermore, embodiments may be implemented by hardware, software, firmware, middleware, microcode, hardware description languages, or any combination thereof. When implemented in software, firmware, middleware or microcode, the program code or code segments to perform the necessary tasks may be stored in a machine readable medium such as storage medium. A processor(s) may perform the necessary tasks. A code segment may represent a procedure, a function, a subprogram, a program, a routine, a subroutine, a module, a software package, a class, or any combination of instructions, data structures, or program statements. A code segment may be coupled to another code segment or a hardware circuit by passing and/or receiving information, data, arguments, parameters, or memory contents. Information, arguments, parameters, data, etc. may be passed, forwarded, or transmitted via any suitable means including memory sharing, message passing, token passing, network transmission, etc.

The foregoing discussion of the invention has been presented for purposes of illustration and description. Further, the description is not intended to limit the invention

to the form disclosed herein. Consequently, variations and modifications commensurate with the above teachings, within the skill or knowledge of the relevant art, are within the scope of the present invention. The embodiments described hereinabove are further intended to explain the best mode presently known of practicing the invention and to enable others skilled in the art to utilize the invention in such or in other embodiments and with various modifications required by the particular application or use of the invention. It is intended that the appended claims be construed to include alternative embodiments to the extent permitted by the prior art.

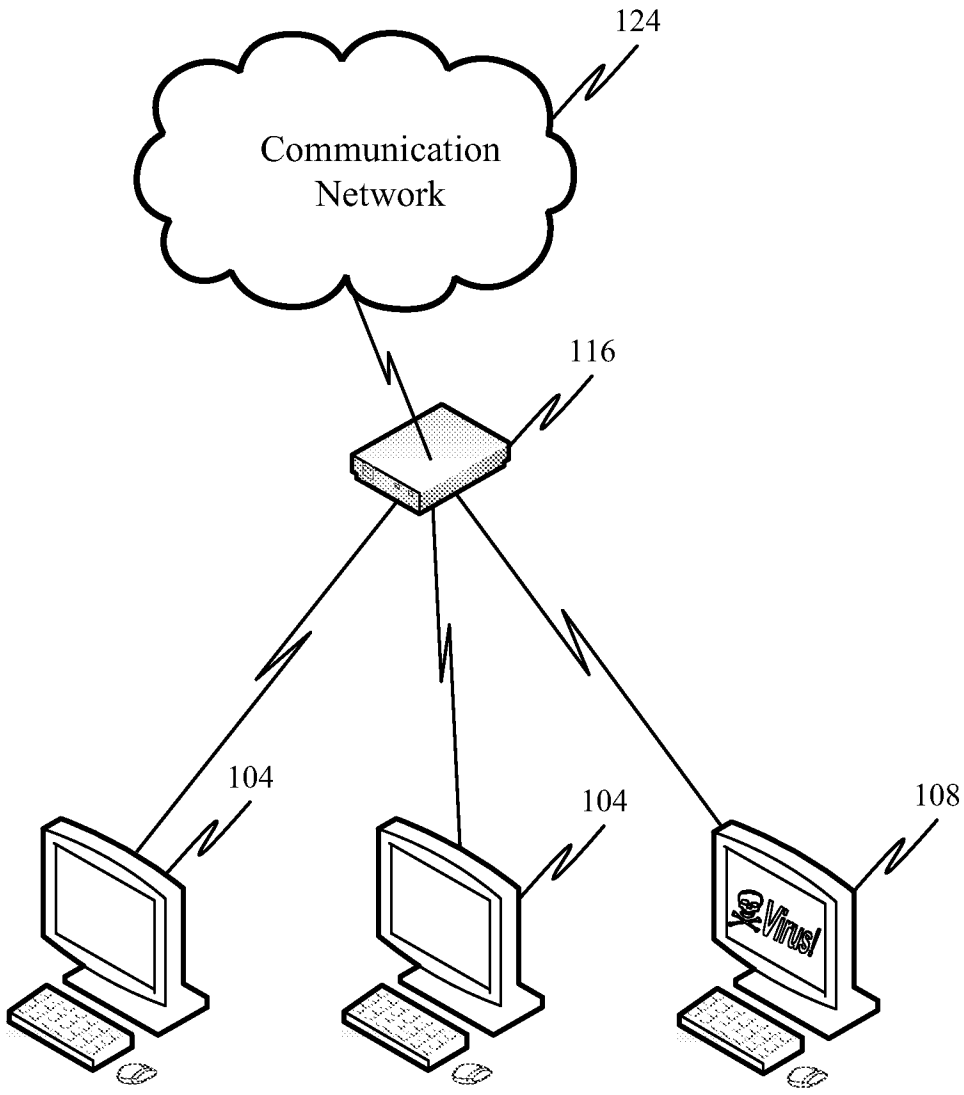


Figure 1

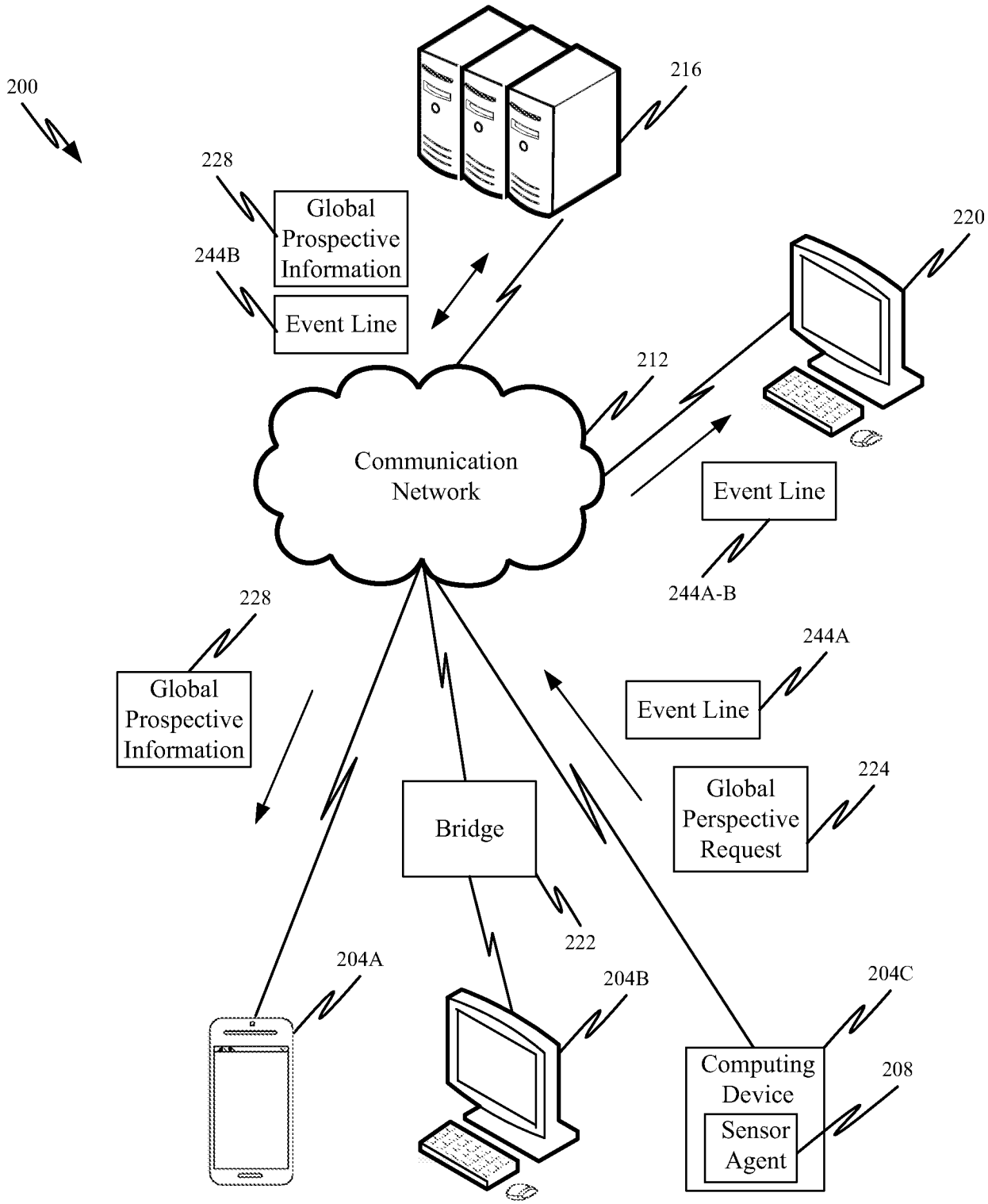

200
216
228
Global Prospective Information
244B
Event Line
220
212
Communication Network
Event Line
244A-B
228
Global Prospective Information
244A
Event Line
224
Global Perspective Request
Bridge
222
204A
204B
204C
Computing Device
208
Sensor Agent

Figure 2

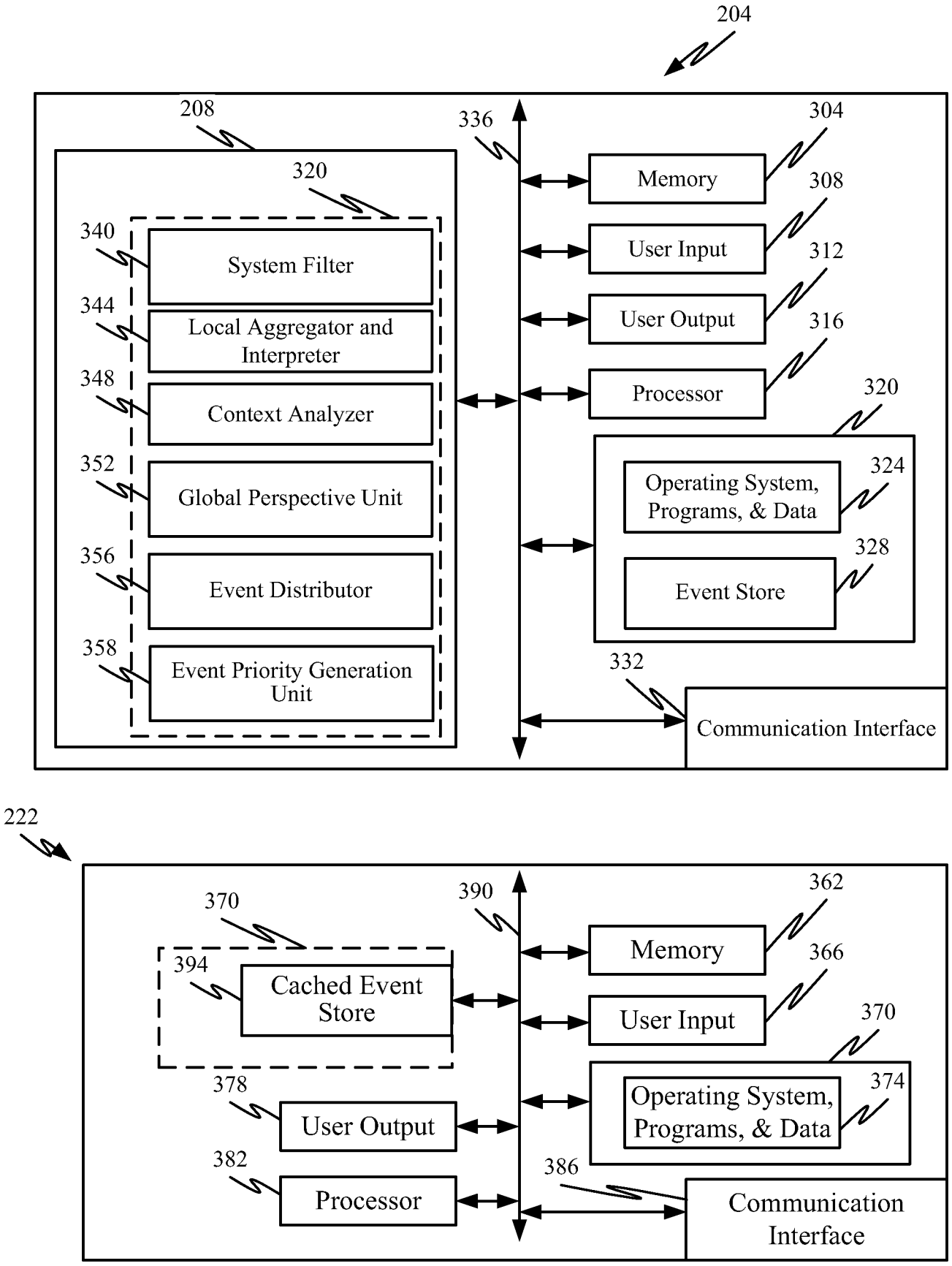

204
208
320
340
System Filter
344
Local Aggregator and Interpreter
348
Context Analyzer
352
Global Perspective Unit
356
Event Distributor
358
Event Priority Generation Unit
336
304
Memory
308
User Input
312
User Output
316
Processor
320
324
Operating System, Programs, & Data
328
Event Store
332
Communication Interface
222
370
394
Cached Event Store
378
User Output
382
Processor
390
362
Memory
366
User Input
370
374
Operating System, Programs, & Data
386
Communication Interface

Figure 3

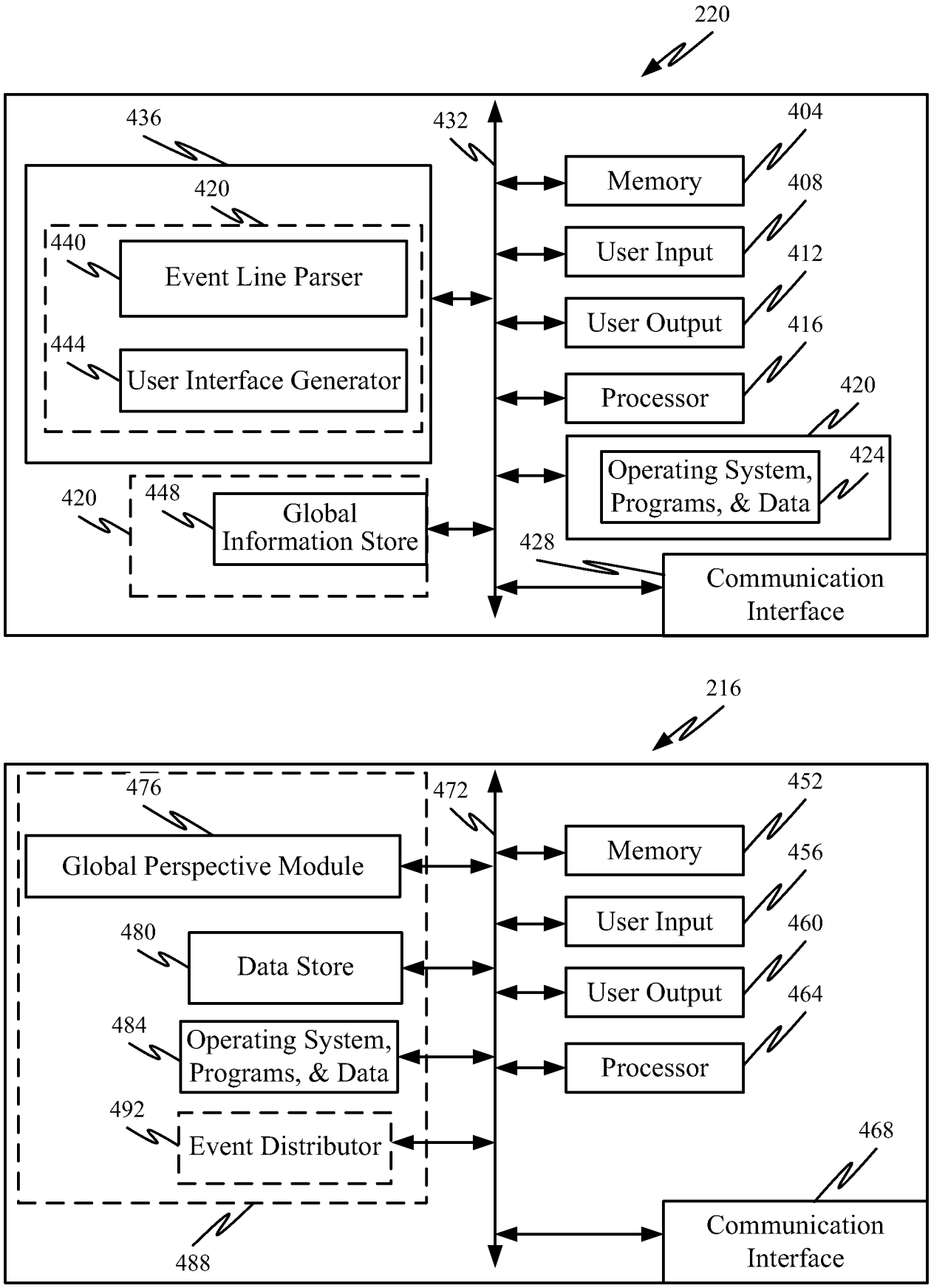

220
436
420
440
Event Line Parser
444
User Interface Generator
420
448
Global Information Store
432
404
Memory
408
User Input
412
User Output
416
Processor
420
424
Operating System, Programs, & Data
428
Communication Interface
216
476
Global Perspective Module
480
Data Store
484
Operating System, Programs, & Data
492
Event Distributor
488
472
452
Memory
456
User Input
460
User Output
464
Processor
468
Communication Interface

Figure 4

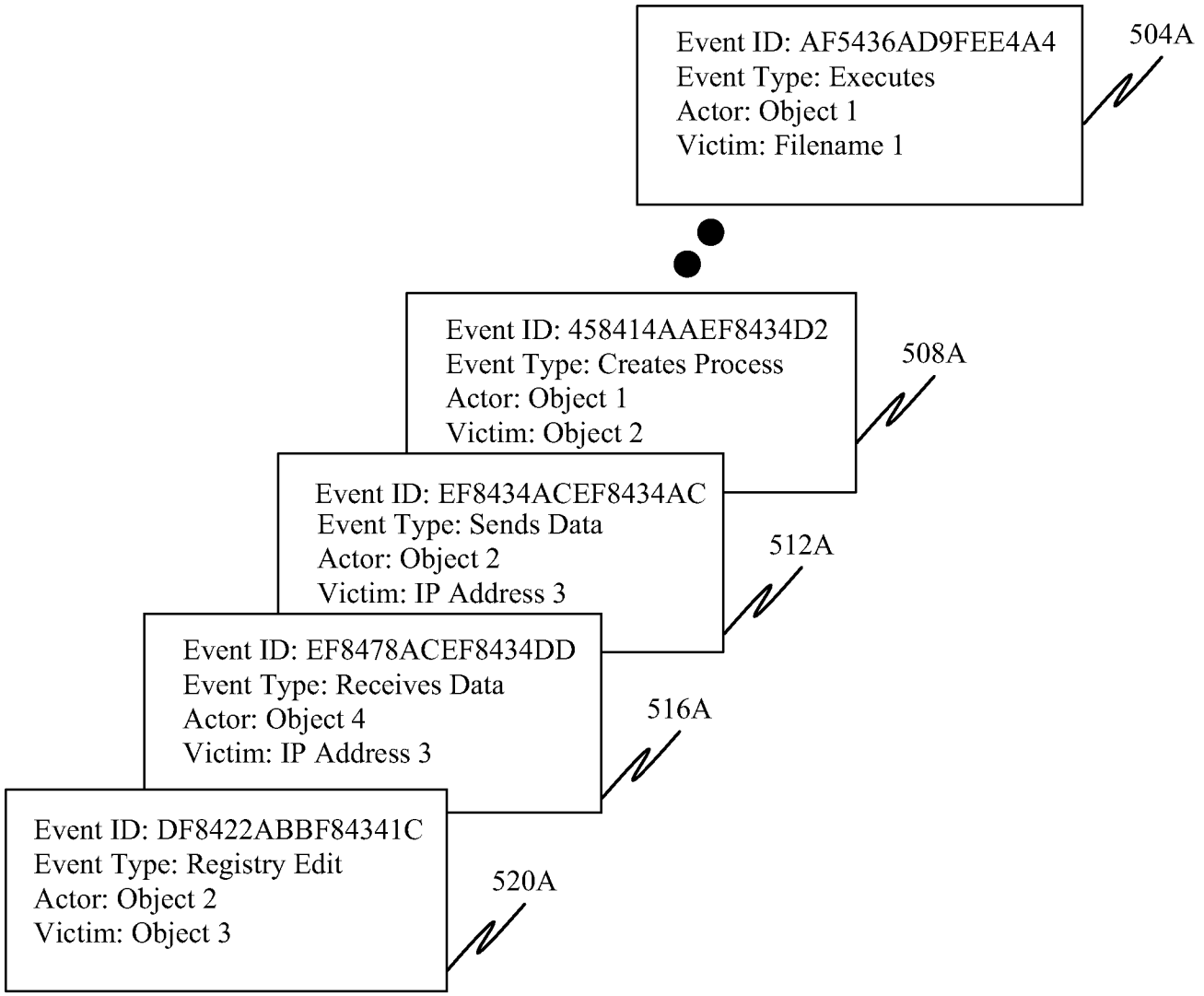

Event ID: AF5436AD9FEE4A4
Event Type: Executes
Actor: Object 1
Victim: Filename 1
504A
Event ID: 458414AAEF8434D2
Event Type: Creates Process
Actor: Object 1
Victim: Object 2
508A
Event ID: EF8434ACEF8434AC
Event Type: Sends Data
Actor: Object 2
Victim: IP Address 3
512A
Event ID: EF8478ACEF8434DD
Event Type: Receives Data
Actor: Object 4
Victim: IP Address 3
516A
Event ID: DF8422ABBF84341C
Event Type: Registry Edit
Actor: Object 2
Victim: Object 3
520A

Figure 5A

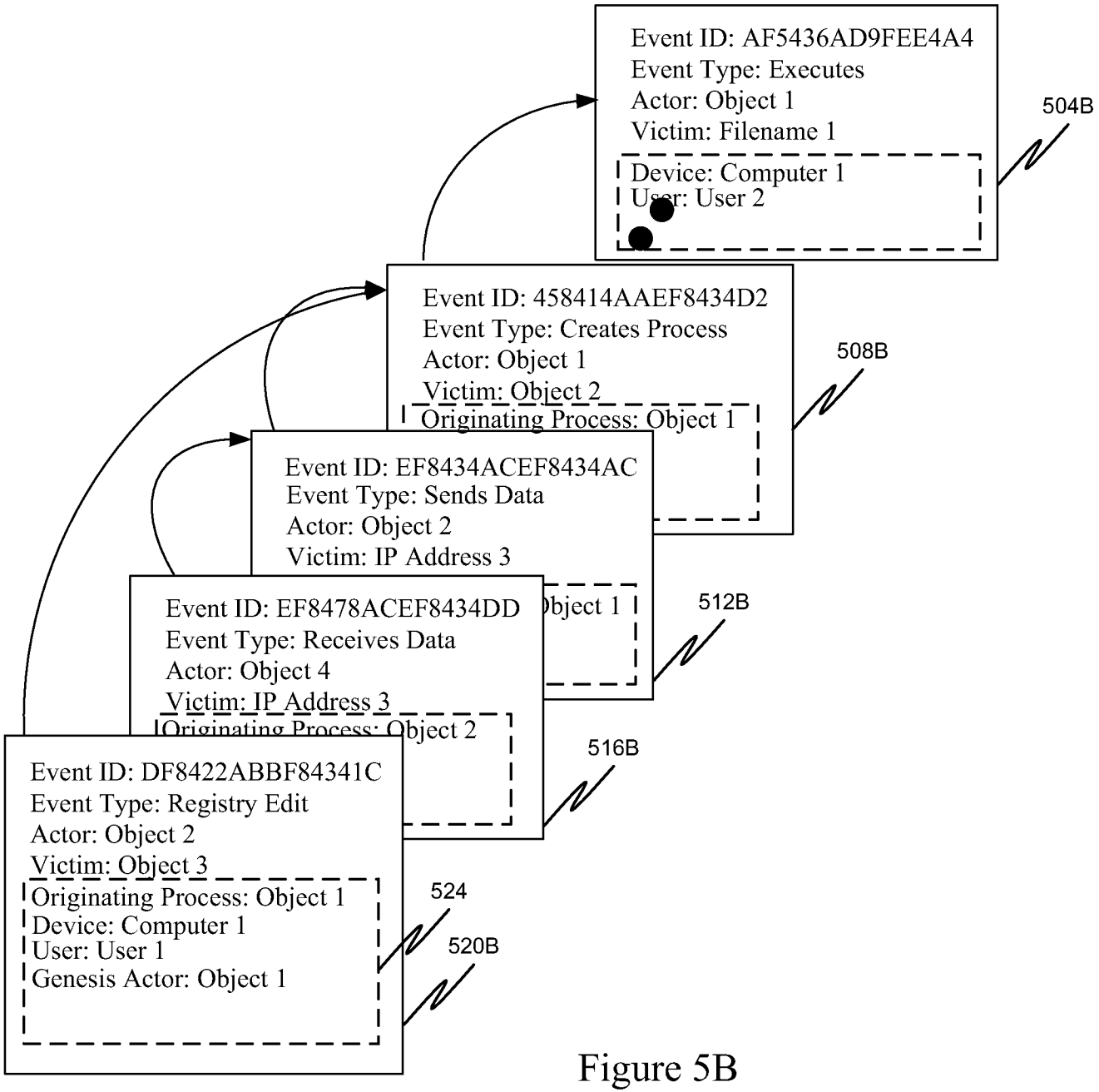

Event ID: AF5436AD9FEE4A4
Event Type: Executes
Actor: Object 1
Victim: Filename 1
Device: Computer 1
User: User 2
504B
Event ID: 458414AAEF8434D2
Event Type: Creates Process
Actor: Object 1
Victim: Object 2
Originating Process: Object 1
508B
Event ID: EF8434ACEF8434AC
Event Type: Sends Data
Actor: Object 2
Victim: IP Address 3
Event ID: EF8478ACEF8434DD
Event Type: Receives Data
Actor: Object 4
Victim: IP Address 3
512B
Event ID: DF8422ABBF84341C
Event Type: Registry Edit
Actor: Object 2
Victim: Object 3
Originating Process: Object 1
Device: Computer 1
User: User 1
Genesis Actor: Object 1
516B
524
520B

Figure 5B

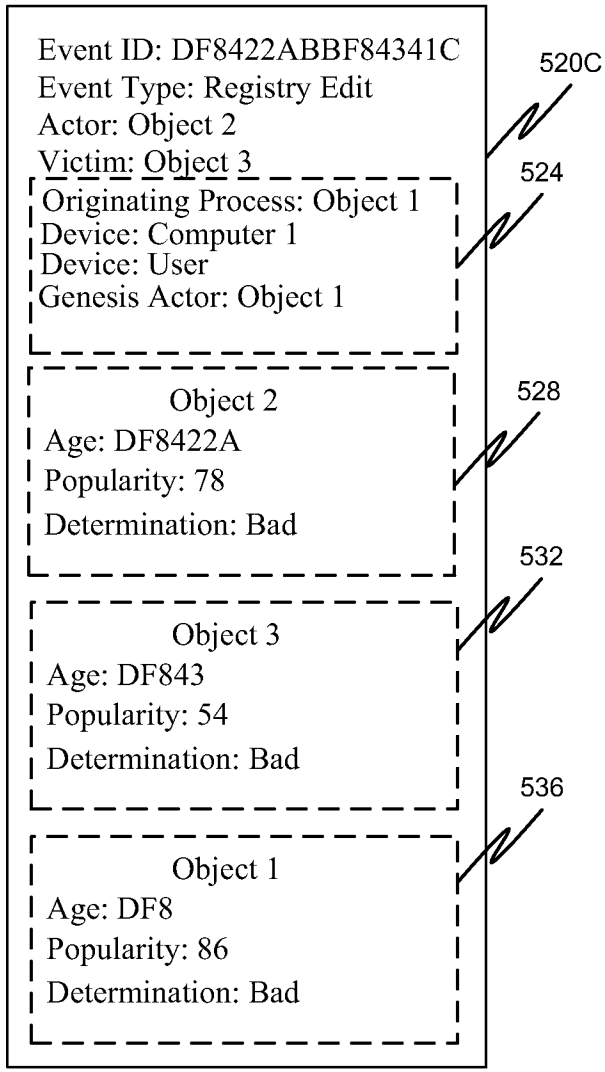

Event ID: DF8422ABBF84341C
Event Type: Registry Edit
Actor: Object 2
Victim: Object 3
520C
Originating Process: Object 1
Device: Computer 1
Device: User
Genesis Actor: Object 1
524
Object 2
Age: DF8422A
Popularity: 78
Determination: Bad
528
Object 3
Age: DF843
Popularity: 54
Determination: Bad
532
Object 1
Age: DF8
Popularity: 86
Determination: Bad
536

Figure 5C

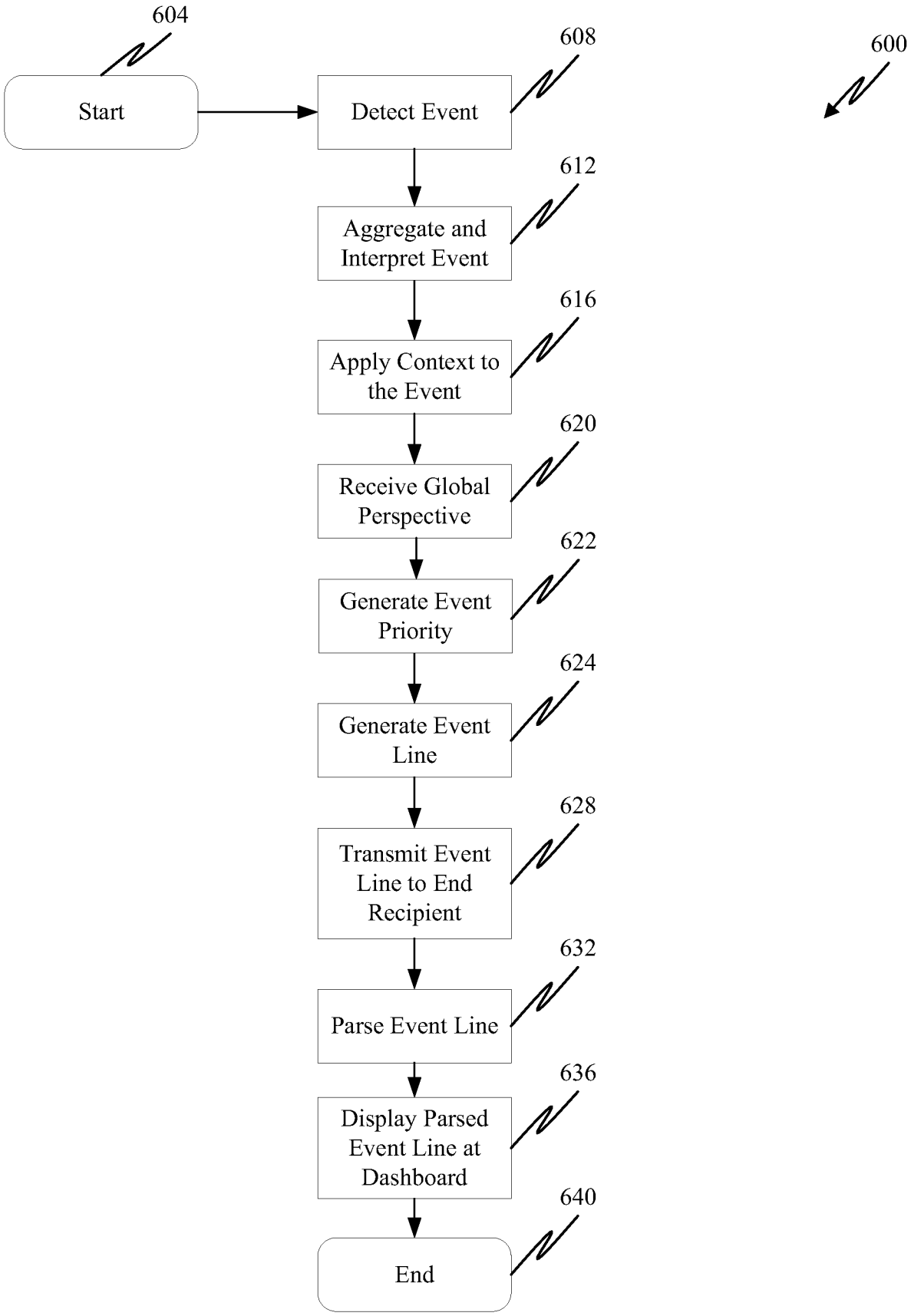

604
Start
608
Detect Event
600
612
Aggregate and Interpret Event
616
Apply Context to the Event
620
Receive Global Perspective
622
Generate Event Priority
624
Generate Event Line
628
Transmit Event Line to End Recipient
632
Parse Event Line
636
Display Parsed Event Line at Dashboard
640
End

Figure 6

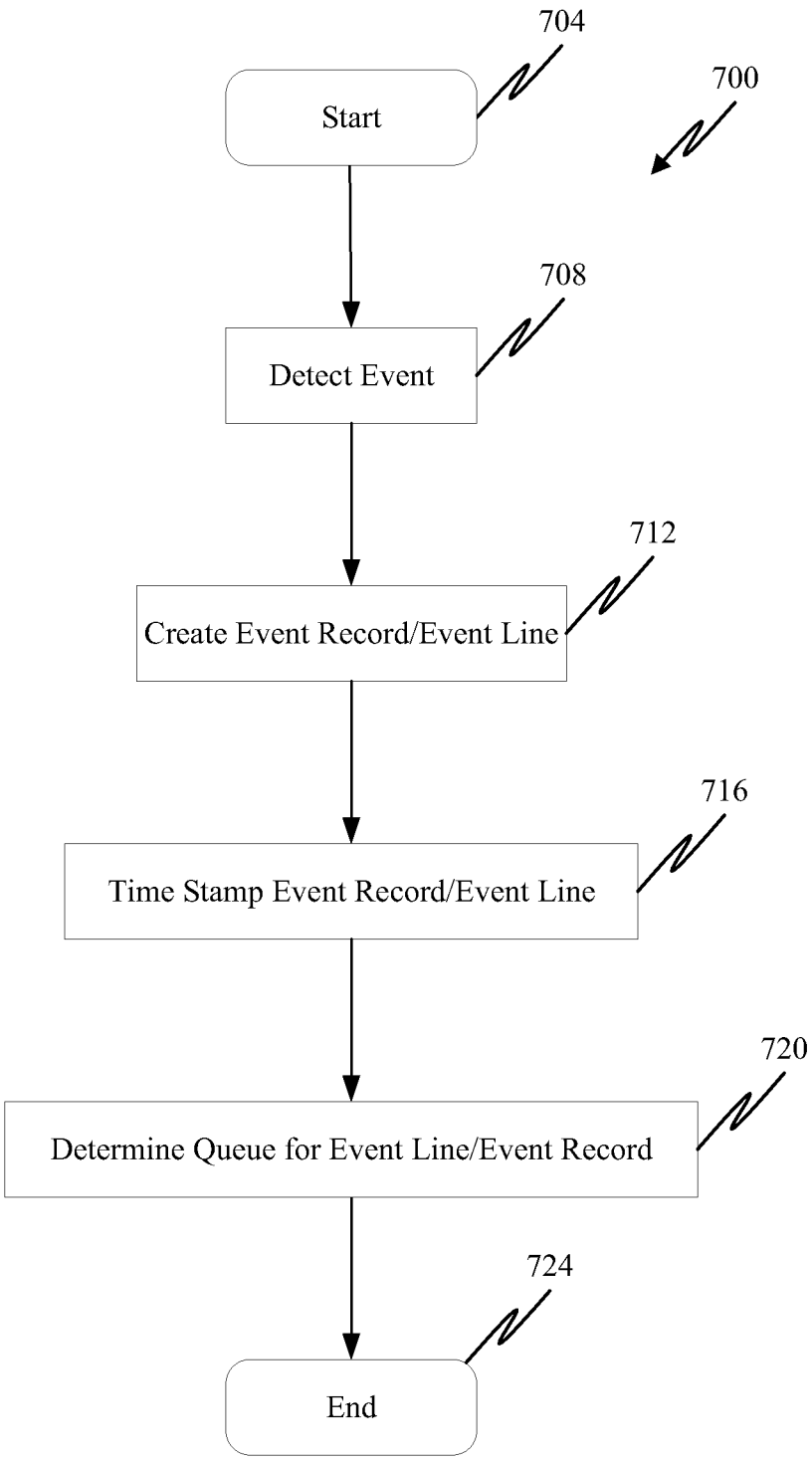

704
700
Start
708
Detect Event
712
Create Event Record/Event Line
716
Time Stamp Event Record/Event Line
720
Determine Queue for Event Line/Event Record
724
End

Figure 7

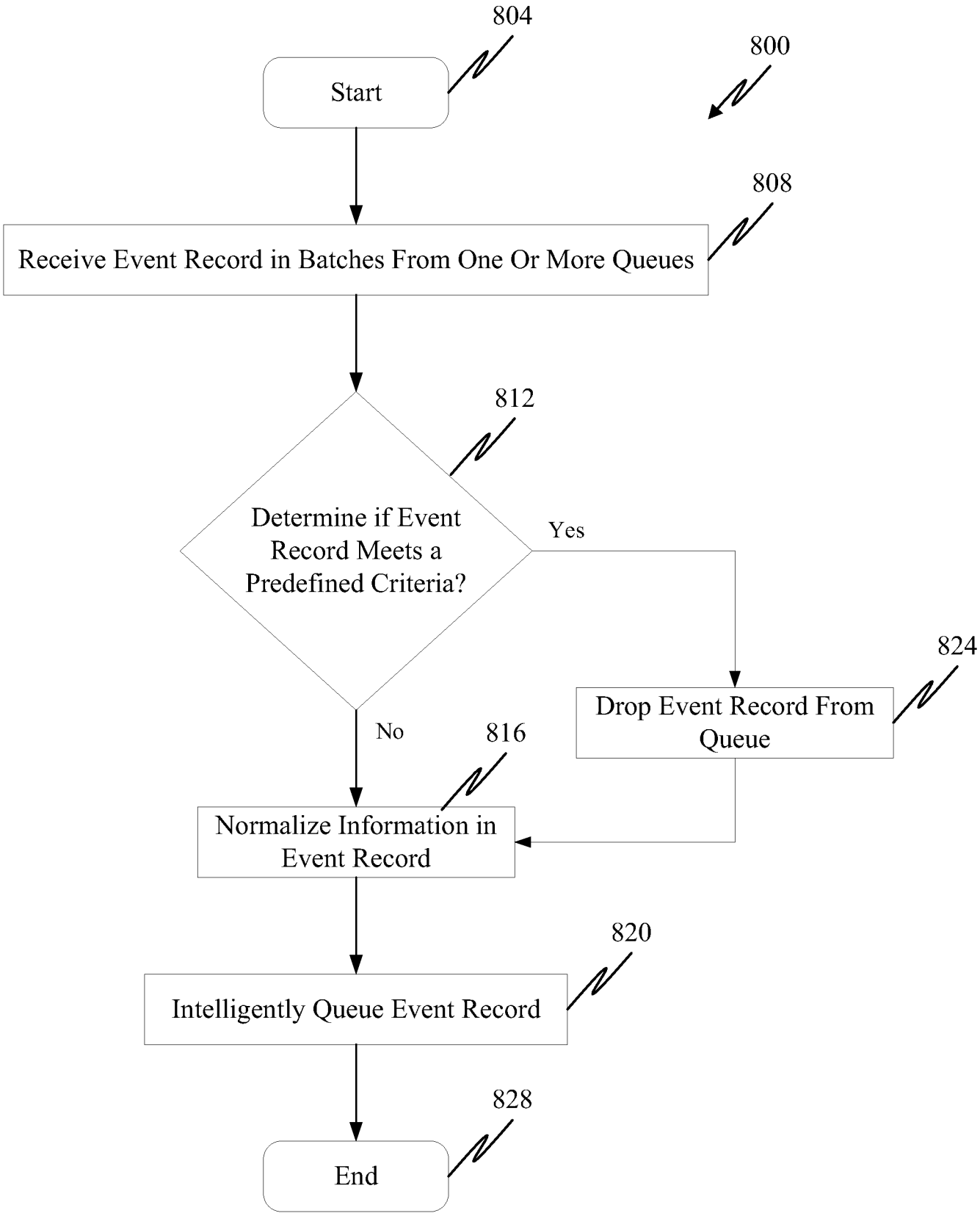

804
800
Start
808
Receive Event Record in Batches From One Or More Queues
812
Determine if Event Record Meets a Predefined Criteria?
Yes
824
Drop Event Record From Queue
No
816
Normalize Information in Event Record
820
Intelligently Queue Event Record
828
End

Figure 8

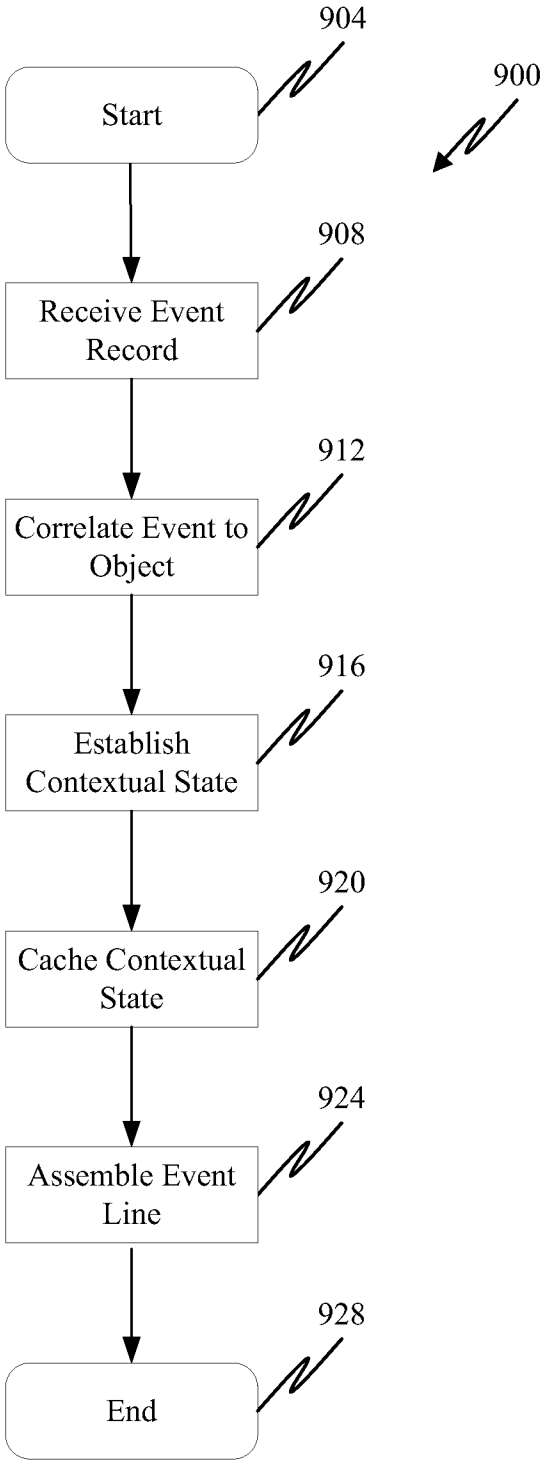

904
900
Start
908
Receive Event Record
912
Correlate Event to Object
916
Establish Contextual State
920
Cache Contextual State
924
Assemble Event Line
928
End

Figure 9

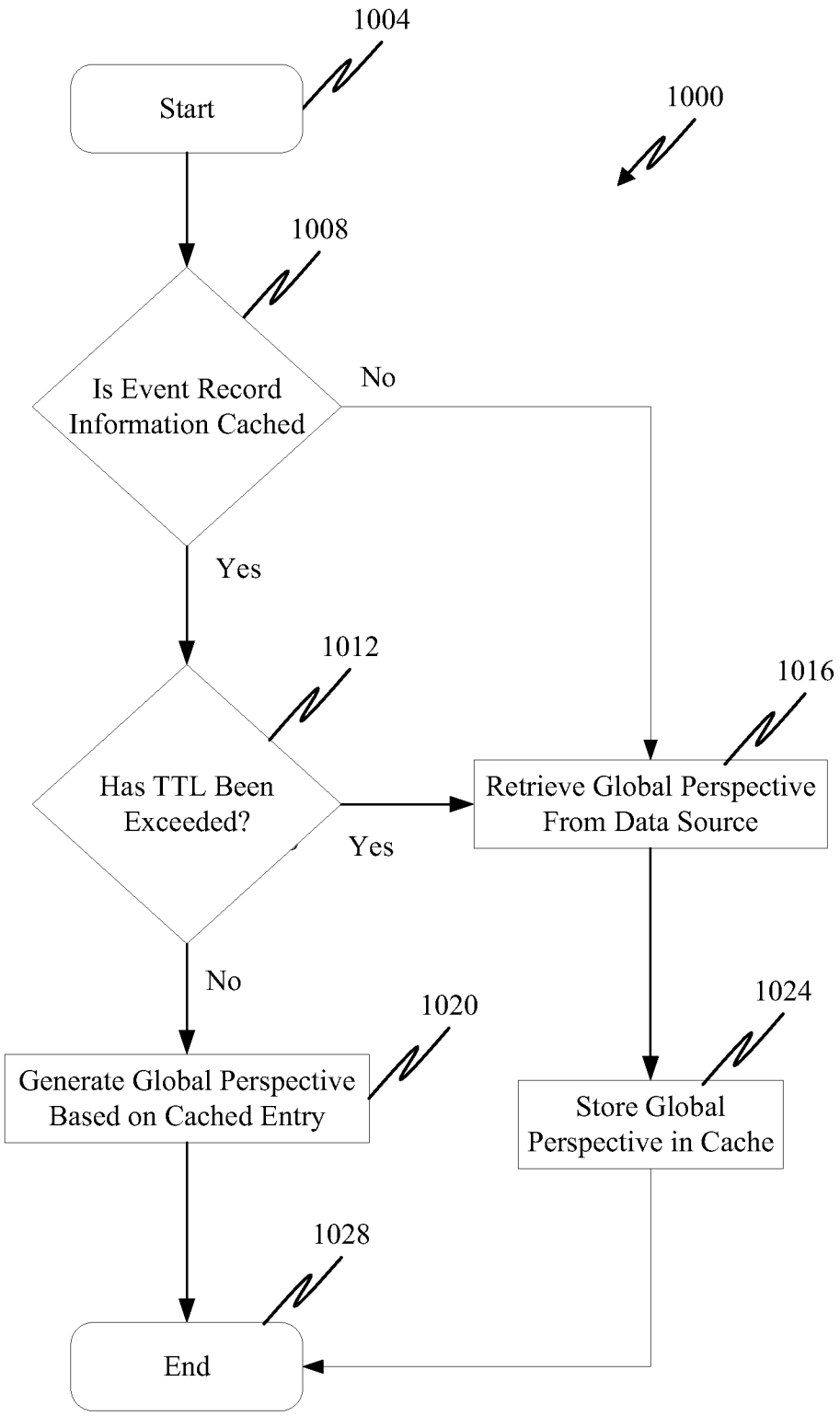

1004
Start
1000
1008
Is Event Record Information Cached
No
Yes
1012
1016
Has TTL Been Exceeded?
Retrieve Global Perspective From Data Source
Yes
No
1020
1024
Generate Global Perspective Based on Cached Entry
Store Global Perspective in Cache
1028
End

Figure 10

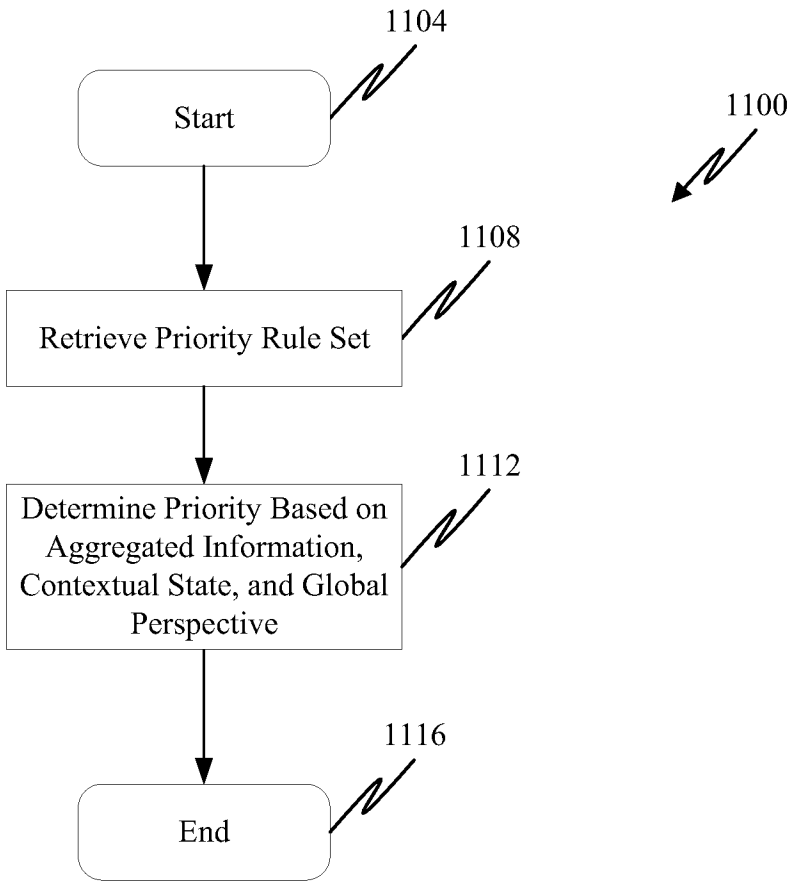

1104
Start
1100
1108
Retrieve Priority Rule Set
1112
Determine Priority Based on Aggregated Information, Contextual State, and Global Perspective
1116
End

Figure 11

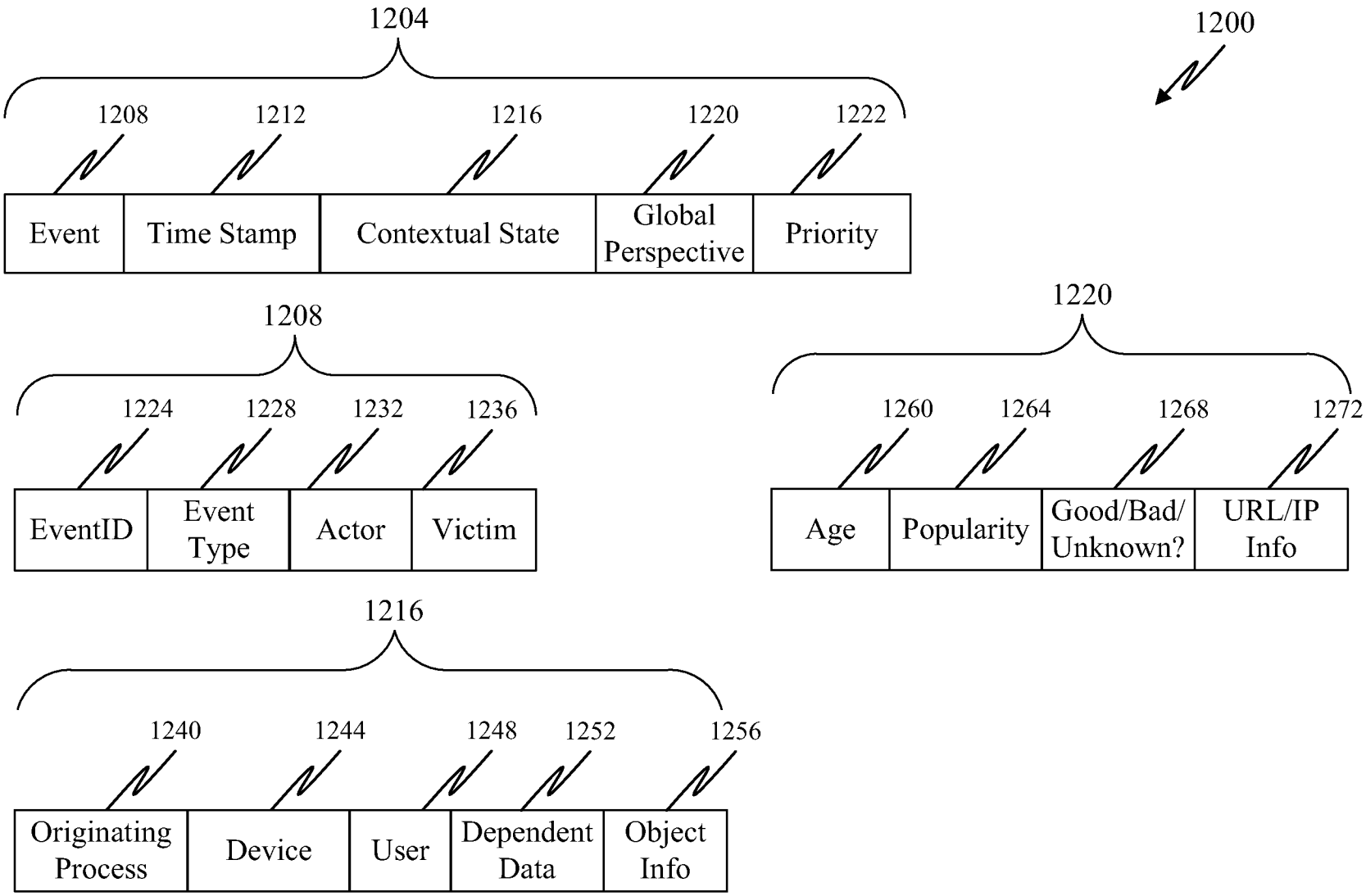

1204
1200
1208
1212
1216
1220
1222
Event
Time Stamp
Contextual State
Global Perspective
Priority
1208
1224
1228
1232
1236
EventID
Event Type
Actor
Victim
1220
1260
1264
1268
1272
Age
Popularity
Good/Bad/ Unknown?
URL/IP Info
1216
1240
1244
1248
1252
1256
Originating Process
Device
User
Dependent Data
Object Info

Figure 12

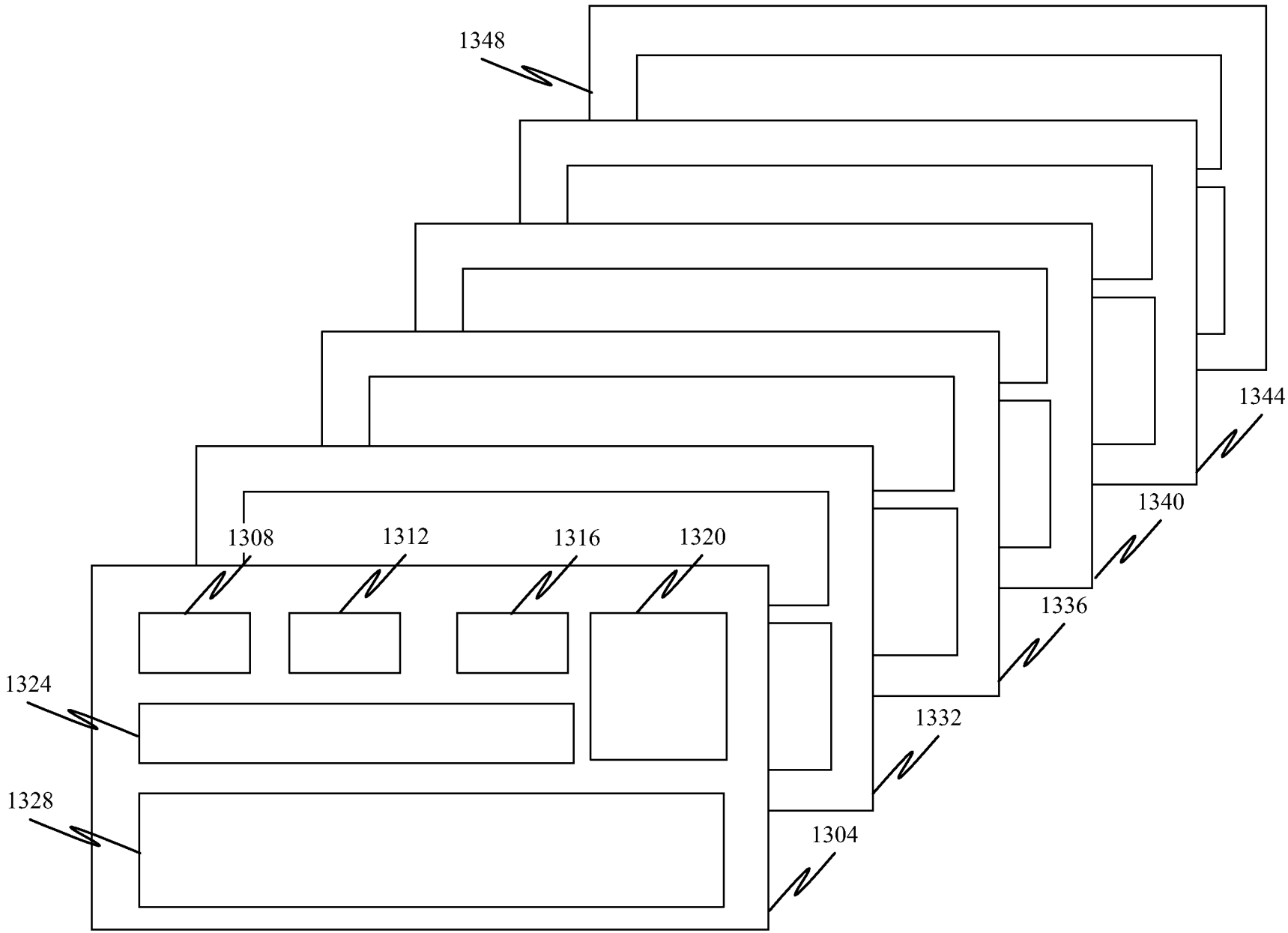


Figure 13

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS

As the below named inventor, I hereby declare that:

This declaration is directed to:

- [x] The attached application, or
- [ ] United States application or PCT international application number _____ filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Joseph A. Jaroch Date (Optional): 5/4/2014

Signature: _____

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS

As the below named inventor, I hereby declare that:

This declaration is directed to:

- [■] The attached application, or
- [ ] United States application or PCT international application number _____ filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Jacques Etienne Erasmus Date (Optional): 05-05-14

Signature: _____

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS

As the below named inventor, I hereby declare that:

This declaration is directed to:

- [■] The attached application, or
- [ ] United States application or PCT international application number _____
  filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Paul Barnes Date (Optional): 7th May 2014

Signature: _____

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS

As the below named inventor, I hereby declare that:

This declaration is directed to:

- [■] The attached application, or
- [ ] United States application or PCT international application number _____

filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Johannes Mayr Date (Optional): May-4th-2014

Signature: _____

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS

As the below named inventor, I hereby declare that:

This declaration is directed to:

- [x] The attached application, or
- [ ] United States application or PCT international application number _____ filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Michael Leidesdorff Date (Optional): 5/5/14

Signature: _____

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/AIA/01 (08-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS

As the below named inventor, I hereby declare that:

This declaration is directed to:

- [■] The attached application, or
- [ ] United States application or PCT international application number _____ filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Marco Giuliani Date (Optional): _____

Signature: _____

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS

As the below named inventor, I hereby declare that:

This declaration is directed to:

- [x] The attached application, or
- [ ] United States application or PCT international application number _____

filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Christopher Jon Williams Date (Optional): _____

Signature: _____

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 3.

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS

As the below named inventor, I hereby declare that:

This declaration is directed to:

- [■] The attached application, or
- [ ] United States application or PCT international application number _____

filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Chad Edward Bacher Date (Optional): 5/4/14

Signature: _____

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

REMARKS

Applicants respectfully request entry of the above amendments in this application prior to examination. This Preliminary Amendment is being submitted to include amendments to the specification. In this Preliminary Amendment, the Specification is being amended to update the priority paragraph. These amendments do not add new matter. Accordingly, Applicants respectfully request that this Preliminary Amendment be entered prior to examination.

It is believed that no additional filing fees are due with this submission. In the event that additional fees are required, the undersigned hereby authorizes the charge of any fees created by the filing of this document or any deficiency of fees submitted herewith to be charged to deposit account no. 13-2725.

Respectfully submitted,

Dated: February 20, 2017

/Andrew T. Pouzeshi/

Andrew T. Pouzeshi, Reg. No. 67,672
Merchant & Gould P.C.
P.O. Box 2903
Minneapolis, MN 55402-0903
(303) 357-1639

23552
PATENT TRADEMARK OFFICE

Amendments to the Specification:

Please amend the first paragraph of the Specification entitled "CROSS-REFERENCE TO RELATED APPLICATION as follows:

CROSS-REFERNCE TO RELATED APPLICATIONS

This application is a continuation application of U.S. Patent Application Serial No. 14/270,069, filed May 5, 2014, which application claims the benefit of U.S. Provisional Patent Application Serial No. 61/819,470, filed May 3, 2013, the entire disclosures of which [[is]] are hereby incorporated herein by reference in their entireties.

PTO/AIA/82A (07-13)
Approved for use through 11/30/2014. OMB 0651-0051
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5, unless the application number and filing date are identified in the Power of Attorney by Applicant form. If neither form PTO/AIA/82A nor form PTO/AIA82B identifies the application to which the Power of Attorney is directed, the Power of Attorney will not be recognized in the application.

Application Number	15/437,275
Filing Date	February 20, 2017
First Named Inventor	Joseph Jaroch
Title	METHOD AND APPARATUS FOR PROVIDING ORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS
Art Unit	Not yet assigned
Examiner Name	Not yet assigned
Attorney Docket Number	04584.0021USC1

SIGNATURE of Applicant or Patent Practitioner

Signature	/Andrew T. Pouzeshi/	Date (Optional)	02/20/2017
Name	Andrew T. Pouzeshi	Registration Number	67672
Title (if Applicant is a juristic entity)	Attorney of Record		
Applicant Name (if Applicant is a juristic entity)	Webroot Inc.		

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. If more than one applicant, use multiple forms.

☐ *Total of _____ forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82B (07-13)
Approved for use through 11/30/2014. OMB 0651-0051
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

POWER OF ATTORNEY BY APPLICANT

I hereby revoke all previous powers of attorney given in the application identified in either the attached transmittal letter or the boxes below.

Application Number	Filing Date

(Note: The boxes above may be left blank if information is provided on form PTO/AIA/82A.)

☑ I hereby appoint the Patent Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above: 23552

OR

☐ I hereby appoint Practitioner(s) named in the attached list (form PTO/AIA/82C) as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the patent application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above. (Note: Complete form PTO/AIA/82C.)

Please recognize or change the correspondence address for the application identified in the attached transmittal letter or the boxes above to:

☑ The address associated with the above-mentioned Customer Number

OR

☐ The address associated with Customer Number:

OR

Firm or Individual Name					
Address					
City		State		Zip	
Country					
Telephone		Email			

I am the Applicant (if the Applicant is a juristic entity, list the Applicant name in the box):

WEBROOT INC.

☐ Inventor or Joint Inventor (title not required below)

☐ Legal Representative of a Deceased or Legally Incapacitated Inventor (title not required below)

☑ Assignee or Person to Whom the Inventor is Under an Obligation to Assign (provide signer's title if applicant is a juristic entity)

☐ Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is concurrently being filed with this document) (provide signer's title if applicant is a juristic entity)

SIGNATURE of Applicant for Patent

The undersigned (whose title is supplied below) is authorized to act on behalf of the applicant (e.g., where the applicant is a juristic entity).

Signature		Date (Optional)	May 12, 2014
Name	Ryan Howe		
Title	Associate General Counsel		

NOTE: Signature - This form must be signed by the applicant in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. If more than one applicant, use multiple forms.

☐ Total of forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Electronic Acknowledgement Receipt

EFS ID:	28405738
Application Number:	15437275
International Application Number:	
Confirmation Number:	4847
Title of Invention:	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS
First Named Inventor/Applicant Name:	Joseph Jaroch
Customer Number:	23552
Filer:	Andrew T. Pouzeshi/Jacquelyn Slate
Filer Authorized By:	Andrew T. Pouzeshi
Attorney Docket Number:	04584.0021USC1
Receipt Date:	20-FEB-2017
Filing Date:	
Time Stamp:	17:27:04
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Power of Attorney	2017-02-20-POA-04584-0021USC1.PDF	403968 43ed25125bd94128ac3113fe5e775819718 82c17	no	2

Warnings:

Information:	
Total Files Size (in bytes):	403968

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Document code: WFEE

United States Patent and Trademark Office
Sales Receipt for Accounting Date: 02/27/2017

ASAHLE	SALE	#00000032	Mailroom Dt:	02/20/2017	132725	15437275	
		01	FC : 1011	280.00	DA		
		02	FC : 1111	600.00	DA		
		03	FC : 1311	720.00	DA		

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 15/437,275

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	280
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	600
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	720
TOTAL CLAIMS (37 CFR 1.16(i))	20 minus 20 =	*			OR	x 80 =	0.00
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*				x 420 =	0.00
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						0.00
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	1600

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
15/437,275	02/20/2017		1600	04584.0021USC1	20	3

CONFIRMATION NO. 4847

23552
MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

FILING RECEIPT

OC000000089319031

Date Mailed: 03/01/2017

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

Joseph Jaroch, Deer Park, IL;
Jacques Etienne Erasmus, Belper, UNITED KINGDOM;
Paul Barnes, Derby, UNITED KINGDOM;
Johannes Mayr, Linz, AUSTRIA;
Michael Leidesdorff, Niwot, CO;
Marco Giuliani, Bastia Umbra, ITALY;
Christopher Jon Williams, Derbyshire, UNITED KINGDOM;
Chad Edward Bacher, Arvada, CO;

Applicant(s)

WEBROOT INC., Broomfield, CO;

Assignment For Published Patent Application

WEBROOT INC., Broomfield, CO

Power of Attorney: The patent practitioners associated with Customer Number 23552

Domestic Priority data as claimed by applicant

This application is a CON of 14/270,069 05/05/2014 PAT 9578045
which claims benefit of 61/819,470 05/03/2013

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 02/27/2017
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 15/437,275**
Projected Publication Date: 06/08/2017
Non-Publication Request: No
Early Publication Request: No
Title

METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS

Preliminary Class

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific

countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop

technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/437,275	02/20/2017	Joseph Jaroch	04584.0021USC1	4847

23552 7590 04/03/2017

MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

EXAMINER	
SHEHNI, GHAZAL B	

ART UNIT	PAPER NUMBER
2436	

NOTIFICATION DATE	DELIVERY MODE
04/03/2017	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

USPTO23552@merchantgould.com

Office Action Summary	Application No. 15/437,275	Applicant(s) JAROCH ET AL.	
	Examiner GHAZAL SHEHNI	Art Unit 2436	AIA (First Inventor to File) Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02/20/2017*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) *1-20* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-20* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *02/20/2017* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

1. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

DETAILED ACTION

Double Patenting Rejections

2. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

3. A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with

this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

4. Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

5. Claims 1-20 are rejected on the ground of nonstatutory double patenting as being unpatentable over claims 1-19 of U.S. Patent No. 9578045. Although the claims at issue are not identical, they are not patentably distinct from each other because Claims of patent application contain every element of claims above instant application or vice versa, and as such they anticipate or anticipated by Instant Application.

Claim Rejections - 35 USC § 112

6. The following is a quotation of 35 U.S.C. 112(b):

> (b) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 5, 11 and 14 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.

8. Claims 5 and 14 recite "...when the global perspective for the at least one event has been cached, obtaining *a global perspective* for the at least one event…". There is insufficient antecedent basis for these limitations. Appropriate correction is required.

9. Claim 11 recites "…an end recipient device, wherein the information associated with…and the sensor agent transmits the event line to *the end recipient*". There is insufficient antecedent basis for these limitations. Appropriate correction is required.

Claim Rejections - 35 USC § 101

10. Claim 8 recites "...a computer readable storage medium...". It appears that the medium recited in the claim 8 is not described in the specification as including a tangible medium in a manner which enables it to act as a computer component to realize the computer program's functionality. Therefore, when the claim is interpreted broadly as transmission medium or signal, the claim appear to be non-statutory because it is not tangibly embodied in a manner so as to be. Examiner suggests to Applicant to amend the claim to include "...at least one non transitory storage medium…" in the claim language. Therefore, the claim 8 is rejected under 35 U.S.C. 101 as being directed to non-statutory subject matter.

Claim Rejections - 35 USC § 112

11. The following is a quotation of 35 U.S.C. 112(d):

> (d) REFERENCE IN DEPENDENT FORMS.—Subject to subsection (e), a claim in dependent form shall contain a reference to a claim previously set forth and then specify a further limitation of the subject matter claimed. A claim in dependent form shall be construed to incorporate by reference all the limitations of the claim to which it refers.

The following is a quotation of 35 U.S.C. 112 (pre-AIA), fourth paragraph:

> Subject to the [fifth paragraph of 35 U.S.C. 112 (pre-AIA)], a claim in dependent form shall contain a reference to a claim previously set forth and then specify a further limitation of the subject matter claimed. A claim in dependent form shall be construed to incorporate by reference all the limitations of the claim to which it refers.

12. Claim 8 is rejected under 35 U.S.C. 112(d) or pre-AIA 35 U.S.C. 112, 4th paragraph, as being of improper dependent form for failing to further limit the subject matter of the claim upon which it depends, or for failing to include all the limitations of the claim upon which it depends. For example, the dependent claim 8, would not conceivably be infringed by anything which would not also infringe the basic claim. Applicant may cancel the claim(s), amend the claim(s) to place the claim(s) in proper dependent form, rewrite the claim(s) in independent form, or present a sufficient showing that the dependent claim(s) complies with the statutory requirements.

Claim Rejections - 35 USC § 103

13. The following is a quotation of 35 U.S.C. 103 which forms the basis for all obviousness rejections set forth in this Office action:

> A patent for a claimed invention may not be obtained, notwithstanding that the claimed invention is not identically disclosed as set forth in section 102, if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains. Patentability shall not be negated by the manner in which the invention was made.

14. Claims 1-20 are rejected under 35 U.S.C. 103 as being unpatentable over Kumar et al (Pub. No. US 2013/0298244) in view of Capalik (Pub. No. US 2008/0016570).

As per claim 1, Kumar discloses a method comprising:
gathering one or more events defining an action of a first object acting on a target

(...receiving temporal events generated by the trust broker that measure the integrity of the system at last scan, and endpoint events from the endpoint trust agent...see par. 114);
generating a contextual state for at least one of the one or more events by correlating the at least one event to an originating object, the contextual state including an indication of the originating object of the first object and an indication of at least one of a device on which the first object is executed and a user associated with the first object (…the system event correlator can be configured to map the events to a cell in the risk correlation matrix grid....and to evaluate threats by category...see par. 114, 116);
obtaining a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object, the information including at least one of age, popularity, a determination as to whether the first object is malware, a determination as to whether the originating object is malware; and Internet Protocol (IP) Address or Uniform Resource Locator (URL) information (…risk correlation matrix illustrates that for each device uniquely identified by a machine identifier (e.g. a virtual machine universally unique identifier, IP address...by mapping alerts to a behavior model threats may be classified...see par. 131). Kumar does not explicitly disclose assembling an event line including details associated with the at least one event, the details including information uniquely identifying each of the first object, the action of the first object, the target, and the originating object; and transmitting the assembled event line. However Capalik disclose **assembling an event line including details associated with the at least one event, the details including information uniquely identifying each of the first object, the action of the first object, the target, and the originating object; and transmitting the assembled event line** (…when an attacker connects to a network port and begins interacting with a virtualized decoy operating system, the introspection module monitors and captures information from the connection, including port numbers, data streams, file uploads, keystrokes, malicious payloads...the captured information containing attack-identifying information, is then sent from the introspection module to the processing module...see par. 48-51). Therefore one ordinary skill in the art would have found it obvious before the effective filling date of the claimed invention to use Capalik in Kumar for including the above limitations because one ordinary skill in the art would recognize it would further enhance detecting intrusion and hence further improving the protection of computer networks, see Capalik, par. 2-3.

As per claim 9, Kumar discloses system for providing forensic visibility into a system, comprising: a device including:
a communication interface; a processor; data storage; and a sensor agent stored on the data storage that is executable by the processor, wherein the sensor agent is operable to:
gather one or more events defining an action of a first object acting on a target
(...receiving temporal events generated by the trust broker that measure the integrity of the system at last scan, and endpoint events from the endpoint trust agent...see par. 114);
generate a contextual state for at least one of the one or more events by correlating the at least one event to an originating object, the contextual state including an indication of the originating object of the first object and an indication of at least one of a device on which the first object is executed and a user associated with the first object (…the system event correlator can be configured to map the events to a cell in the risk correlation matrix

grid....and to evaluate threats by category...see par. 114, 116);
obtain a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object, the information including at least one of age, popularity, a determination as to whether the first object is malware, a determination as to whether the originating object is malware; and Internet Protocol (IP) Address or Uniform Resource Locator (URL) information (…risk correlation matrix illustrates that for each device uniquely identified by a machine identifier (e.g. a virtual machine universally unique identifier, IP address...by mapping alerts to a behavior model threats may be classified...see par. 131). Kumar does not explicitly disclose assemble an event line including details associated with the at least one event, the details including information uniquely identifying each of the first object, the action of the first object, the target, and the originating object; and transmit the assembled event line utilizing the communication interface. However Capalik disclose **assemble an event line including details associated with the at least one event, the details including information uniquely identifying each of the first object, the action of the first object, the target, and the originating object; and transmit the assembled event line utilizing the communication interface** (…when an attacker connects to a network port and begins interacting with a virtualized decoy operating system, the introspection module monitors and captures information from the connection, including port numbers, data streams, file uploads, keystrokes, malicious payloads...the captured information containing attack-identifying information, is then sent from the introspection module to the processing module...see par. 48-51). Therefore one ordinary skill in the art would have found it obvious before the effective filling date of the claimed invention to use Capalik in Kumar for including the above limitations because one ordinary skill in the art would recognize it would further enhance detecting intrusion and hence further improving the protection of computer networks, see Capalik, par. 2-3.

As per claim 17, Kumar discloses system for providing forensic visibility into a system, comprising: a device including: a communication interface; a processor; data storage; and a sensor agent stored on the data storage that is executable by the processor, wherein the sensor agent is operable to: gather one or more events defining an action of a first object acting on a target (...receiving temporal events generated by the trust broker that measure the integrity of the system at last scan, and endpoint events from the endpoint trust agent...see par. 114);
generate a contextual state for at least one of the one or more events by correlating the at least one event to an originating object, the contextual state including an indication of the originating object of the first object and an indication of at least one of a device on which the first object is executed and a user associated with the first object (…the system event correlator can be configured to map the events to a cell in the risk correlation matrix grid....and to evaluate threats by category...see par. 114, 116). Kumar does not explicitly disclose assemble an event line including details associated with the at least one event, the details including information uniquely identifying each of the first object, the action of the first object, the target, and the originating object; and transmit the assembled event line utilizing the communication interface. However Capalik disclose **assemble an event line including details associated with the at least one event, the details including information uniquely identifying each of the first object, the action of the first object, the target, and the**

originating object; and transmit the assembled event line utilizing the communication interface (…when an attacker connects to a network port and begins interacting with a virtualized decoy operating system, the introspection module monitors and captures information from the connection, including port numbers, data streams, file uploads, keystrokes, malicious payloads...the captured information containing attack-identifying information, is then sent from the introspection module to the processing module...see par. 48-51). Therefore one ordinary skill in the art would have found it obvious before the effective filling date of the claimed invention to use Capalik in Kumar for including the above limitations because one ordinary skill in the art would recognize it would further enhance detecting intrusion and hence further improving the protection of computer networks, see Capalik, par. 2-3.

As per claim 2, the combination of Kumar and Capalik discloses wherein the information associated with the one or more of the first object and the originating object is obtained from a community database; and wherein the event line is transmitted to an end recipient (Kumar: see par. 140-141).

As per claim 3, the combination of Kumar and Capalik discloses obtaining an event priority based on one or more of the generated context and the global perspective for the at least one event, wherein the event line further includes the event priority for the at least one event (Kumar: see par. 159).

As per claim 4, the combination of Kumar and Capalik discloses wherein the at least one event includes information uniquely identifying the object performing the action, information uniquely identifying the action being performed, and information uniquely identifying the target upon which the act is being performed (Kumar: see par. 131).

As per claim 5, the combination of Kumar and Capalik discloses determining whether a global perspective for the at least one event has been cached; when the global perspective for the at least one event has been cached, obtaining a global perspective for the at least one event based on the cached global perspective; and when the global perspective for the at least one event has not been cached, obtaining a global perspective for the at least one event from a community database (Kumar: see par. 169, 174).

As per claim 6, the combination of Kumar and Capalik discloses determining whether the cached global perspective for the at least one event has expired; and when the global perspective for the at least one event has expired, obtaining a global perspective for the at least one event from a community database (Kumar: see par. 68, 83).

As per claim 7, the combination of Kumar and Capalik discloses heuristically displaying information identifying the first object performing the action, information identifying the action being performed, information identifying the target upon which the act is being performed, and the global perspective according to one or more of a location associated with the first object; at least one characteristic of an outbound connection associated with the first object; a dropped executable file; an age of the first object; and a number of concurrent connections associated

with the first object (Kumar: see par. 131, 169, 171).

Claim 8 is reject under the same grounds of rejections as in claim 1.

As per claim 10, the combination of Kumar and Capalik discloses wherein the at least one of the one or more events is executed by the processor (Kumar: see par. 169, 171).

As per claim 11, the combination of Kumar and Capalik discloses a global perspective information server; and an end recipient device, wherein the information associated with the one or more of the first object and the originating object is obtained from the global perspective information server and the sensor agent transmits the event line to the end recipient (Kumar: see par. 140-141).

As per claim 12, the combination of Kumar and Capalik discloses wherein the sensor agent is further operable to: cache the one or more events; and asynchronously consolidate and normalize the one or more events (Kumar: see par. 307).

As per claim 13, the combination of Kumar and Capalik discloses wherein the at least one event includes information uniquely identifying the object performing the action, information uniquely identifying the action being performed, and information uniquely identifying the target upon which the act is being performed (Kumar: see par. 131).

As per claim 14, the combination of Kumar and Capalik discloses wherein the sensor agent is further operable to: determine whether a global perspective for the at least one event has been cached; when the global perspective for the at least one event has been cached, obtain a global perspective for the at least one event based on the cached global perspective; and when the global perspective for the at least one event has not been cached, obtain a global perspective for the at least one event from a community database (Kumar: see par. 169, 174).

As per claim 15, the combination of Kumar and Capalik discloses wherein the sensor agent is further operable to: determine whether the cached global perspective for the at least one event has expired; and when the global perspective for the at least one event has expired, obtain a global perspective for the at least one event from a community database (Kumar: see par. 68, 83).

As per claim 16, the combination of Kumar and Capalik discloses wherein the end recipient heuristically displays information identifying the first object performing the action, information identifying the action being performed, information identifying the target upon which the act is being performed, and the global perspective according to one or more of a location associated with the first object; at least one characteristic of an outbound connection associated with the first object; a dropped executable file; an age of the first object; and a number of concurrent connections associated with the first object (Kumar: see par. 131, 169, 171).

As per claim 18, the combination of Kumar and Capalik discloses a global perspective information server including: a processor; a communication interface; data storage; and a global perspective

module, wherein the global perspective module is operable to: receive the event line from the device (Kumar: the system event correlator can be configured to map the events to a cell in the risk correlation matrix grid....and to evaluate threats by category...see par. 114, 116); **obtain a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object, the information including at least one of age, popularity, a determination as to whether the first object is malware, a determination as to whether the originating object is malware; and Internet Protocol (IP) Address or Uniform Resource Locator (URL) information** (Kumar: risk correlation matrix illustrates that for each device uniquely identified by a machine identifier (e.g. a virtual machine universally unique identifier, IP address...by mapping alerts to a behavior model threats may be classified...see par. 131); **assemble a second event line including details associated with the at least one event, the details including information uniquely identifying each of the first object, the action of the first object, the target, and the originating object; and transmit the assembled second event line utilizing the communication interface to an end recipient** (Capalik: when an attacker connects to a network port and begins interacting with a virtualized decoy operating system, the introspection module monitors and captures information from the connection, including port numbers, data streams, file uploads, keystrokes, malicious payloads...the captured information containing attack-identifying information, is then sent from the introspection module to the processing module...see par. 48-51).

As per claim 19, the combination of Kumar and Capalik discloses wherein the end recipient heuristically displays information identifying the first object performing the action, information identifying the action being performed, information identifying the target upon which the act is being performed, and the global perspective according to one or more of a location associated with the first object; at least one characteristic of an outbound connection associated with the first object; a dropped executable file; an age of the first object; and a number of concurrent connections associated with the first object (Kumar: see par. 131, 169, 171).

As per claim 20, the combination of Kumar and Capalik discloses a bridge including: a processor; a communication interface; and a cached event store, wherein the cached event store is operable to: receive a first request for a global perspective for the at least one event; receive a second request for a global perspective for another event, the second request originating from another device; obtain a first global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object, the information including at least one of age, popularity, a determination as to whether the first object is malware, a determination as to whether the originating object is malware; and Internet Protocol (IP) Address or Uniform Resource Locator (URL) information; obtain a second global perspective for the another event; provide the first global perspective to the device; and provide the second global perspective to the another device (Capalik: see par. 45).

Conclusion

15. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure (see PTO-form 892).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to GHAZAL SHEHNI whose telephone number is (571)270-7479. The examiner can normally be reached on Monday-Thursday.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gelagay Shewaye can be reached on (571)272-4219. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/GHAZAL SHEHNI/
Primary Examiner, Art Unit 2436

Notice of References Cited	Application/Control No. 15/437,275	Applicant(s)/Patent Under Reexamination JAROCH ET AL.	
	Examiner GHAZAL SHEHNI	Art Unit 2436	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-2013/0298244 A1	11-2013	KUMAR; Srinivas	G06F21/52	726/25
*	B	US-2008/0016570 A1	01-2008	Capalik; Alen	H04L63/1408	726/23
*	C	US-2013/0247201 A1	09-2013	Alperovitch; Dmitri	H04L63/14	726/24
	D	US-				
	E	US-				
	F	US-				
	G	US-				
	H	US-				
	I	US-				
	J	US-				
	K	US-				
	L	US-				
	M	US-				

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 4847

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
15/437,275	02/20/2017	726	2436	04584.0021USC1

APPLICANTS

WEBROOT INC., Broomfield, CO;

INVENTORS

Joseph Jaroch, Deer Park, IL;
Jacques Etienne Erasmus, Belper, UNITED KINGDOM;
Paul Barnes, Derby, UNITED KINGDOM;
Johannes Mayr, Linz, AUSTRIA;
Michael Leidesdorff, Niwot, CO;
Marco Giuliani, Bastia Umbra, ITALY;
Christopher Jon Williams, Derbyshire, UNITED KINGDOM;
Chad Edward Bacher, Arvada, CO;

**** CONTINUING DATA ***************************

This application is a CON of 14/270,069 05/05/2014 PAT 9578045
which claims benefit of 61/819,470 05/03/2013

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ****

02/27/2017

Foreign Priority claimed	35 USC 119(a-d) conditions met	Verified and Acknowledged	Met after Allowance	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
☐ Yes ☑ No	☐ Yes ☑ No	/GHAZAL B SHEHNI/ Examiner's Signature	☐ Initials	IL	15	20	3

ADDRESS

MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903
UNITED STATES

TITLE

METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS

FILING FEE RECEIVED		
1600	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15437275	JAROCH ET AL.
	Examiner	**Art Unit**
	GHAZAL SHEHNI	2436

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	03/28/2017								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	880	(virus or malicious or trojan or spy$ware or mal$ware) with ((analyz$3 or analys$3 or determin$5 or detect$4) with (security with event))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/28 14:17
L2	21	(virus or malicious or trojan or spy$ware or mal$ware) with (((analyz$3 or analys$3 or determin$5 or detect$4) with forensic) with (security with (behavior or pattern or event)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/28 14:22
L3	17254	(analys$3 or analyz$3 or detect$4 or monitor$3 or record$3 or captur$3) with ((security with attack) or (network with attack))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/28 14:26
L4	213	(analys$3 or analyz$3 or detect$4 or monitor$3 or record$3 or captur$3) with ((security with attack) or (network with attack)) with forensic	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/28 14:26
L5	111	4 AND ((H04L63/1416 OR H04L63/20 OR H04L63/1425 OR H04L63/1441 OR H04L63/1408 OR H04L63/1433 OR H04L63/145 OR H04L63/14 OR H04L9/3271 OR H04L12/2602).CPC.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/28 14:29
L6	1	("20130298244").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2017/03/28 14:32
S1	10	(("JAROCH") near3 ("Joseph")).INV.	US-PGPUB; USPAT; USOCR	ADJ	ON	2017/03/27 20:14
S2	3	(("ERASMUS") near3 ("Jacques")).INV.	US-PGPUB; USPAT; USOCR	ADJ	ON	2017/03/27 20:14
S3	63	(("BARNES") near3 ("Paul")).INV.	US-PGPUB; USPAT; USOCR	ADJ	ON	2017/03/27 20:14
S4	9	(("MAYR") near3 ("Johannes")).INV.	US-PGPUB; USPAT; USOCR	ADJ	ON	2017/03/27 20:15
S5	2	(("LEIDESDORFF") near3 ("Michael")).INV.	US-PGPUB; USPAT; USOCR	ADJ	ON	2017/03/27 20:15
S6	16	(("GIULIANI") near3 ("Marco")).INV.	US-PGPUB;	ADJ	ON	2017/03/27

			USPAT; USOCR			20:15
S7	1533	(("WILLIAMS") near3 ("Christopher")).INV.	US-PGPUB; USPAT; USOCR	ADJ	ON	2017/03/27 20:15
S8	2	(("BACHER") near3 ("Chad")).INV.	US-PGPUB; USPAT; USOCR	ADJ	ON	2017/03/27 20:15

EAST Search History (Interference)

< This search history is empty>

3/28/2017 3:27:59 PM
C:\Users\gshehni\Documents\EAST\Workspaces\15437275.wsp

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15437275	JAROCH ET AL.
	Examiner	Art Unit
	GHAZAL SHEHNI	2436

CPC- SEARCHED		
Symbol	Date	Examiner
H04L63/1416 OR H04L63/20 OR H04L63/1425 OR H04L63/1441 OR H04L63/1408 OR H04L63/1433 OR H04L63/145 OR H04L63/14 OR H04L9/3271 OR H04L12/2602	3/28/2017	GS

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor search (see search history printout)	3/28/2017	GS
East (see search history printout)	3/28/2017	GS
CPC with text search	3/28/2017	GS

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

	/GHAZAL SHEHNI/ Primary Examiner, Art Unit 2436

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
15/437,275	02/20/2017	Joseph Jaroch	04584.0021USC1

CONFIRMATION NO. 4847

23552
MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

PUBLICATION NOTICE

OC000000091945450

Title:METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS

Publication No.US-2017-0163660-A1
Publication Date:06/08/2017

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (571) 272-3150 or (800) 972-6382, by facsimile at (571) 273-3250, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

PTO/SB/08a (03-15)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	15437275
Filing Date	2017-02-20
First Named Inventor	Joseph Jaroch
Art Unit	2436
Examiner Name	SHEHNI, GHAZAL B
Attorney Docket Number	04584.0021USC1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	7895649		2011-02-22	Brook et al.	
	2	9578045		2017-02-21	Jaroch et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20060095963		2006-05-04	Crosby et al.	
	2	20080244694		2008-10-02	Neystadt et al.	
	3	20090300769		2009-12-03	Srinivasa et al.	
	4	20120072725		2012-03-22	Fanton et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15437275
	Filing Date	2017-02-20
	First Named Inventor	Joseph Jaroch
	Art Unit	2436
	Examiner Name	SHEHNI, GHAZAL B
	Attorney Docket Number	04584.0021USC1

	5	20120260340		2012-10-11	Morris et al.			

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	2006094228	WO		2006-09-08	Shull et al.		
	2	2012110501	WO		2012-08-23	Morris et al.		

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	European Extended Search Report in Application 14791882.5, mailed 2016-11-11, 8 pages.	
	2	PCT International Preliminary Report on Patentability in PCT/US2014/036832, mailed 2015-11-03, 8 pages.	
	3	PCT International Search Report in PCT/US2014/036832, mailed 2014-09-29, 9 pages.	
	4	US Patent Application 14/270,069, Amendment and Response filed 2016-03-16, 16 pages.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15437275
	Filing Date	2017-02-20
	First Named Inventor	Joseph Jaroch
	Art Unit	2436
	Examiner Name	SHEHNI, GHAZAL B
	Attorney Docket Number	04584.0021USC1

	5	US Patent Application 14/270,069, Amendment and Response filed 2016-08-31, 13 pages.	
	6	US Patent Application 14/270,069, Notice of Allowance mailed 2016-10-05, 8 pages.	
	7	US Patent Application 14/270,069, Office Action mailed 2015-09-16, 12 pages.	
	8	US Patent Application 14/270,069, Office Action mailed 2016-05-31, 11 pages.	

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15437275
	Filing Date	2017-02-20
	First Named Inventor	Joseph Jaroch
	Art Unit	2436
	Examiner Name	SHEHNI, GHAZAL B
	Attorney Docket Number	04584.0021USC1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Andrew T. Pouzeshi/	Date (YYYY-MM-DD)	2017-08-21
Name/Print	Andrew T. Pouzeshi	Registration Number	67672

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 September 2006 (08.09.2006)

PCT

(10) International Publication Number
WO 2006/094228 A2

(51) International Patent Classification: Not classified

(21) International Application Number:
PCT/US2006/007728

(22) International Filing Date: 2 March 2006 (02.03.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/658,124	2 March 2005 (02.03.2005)	US
60/658,087	2 March 2005 (02.03.2005)	US
60/658,281	2 March 2005 (02.03.2005)	US

(71) Applicant *(for all designated States except US)*: **MARKMONITOR, INC.** [US/US]; Emerald Tech Center, 391 N. Ancestor Place, Boise, Idaho 83704 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **SHULL, Mark** [US/US]; 203 Oxford Street, Chevy Chase, Maryland 20815 (US). **BOHLMAN, William** [US/US]; 4350 N. West View Way, Boise, Idaho 83704 (US). **SHRAIM, Ihab** [US/US]; 13307 Queenstown Lane, Germantown, Maryland 20874 (US). **BURA, Christopher, J.** [US/US]; 41 Carpenter Court, Pleasant Hill, California 94523 (US).

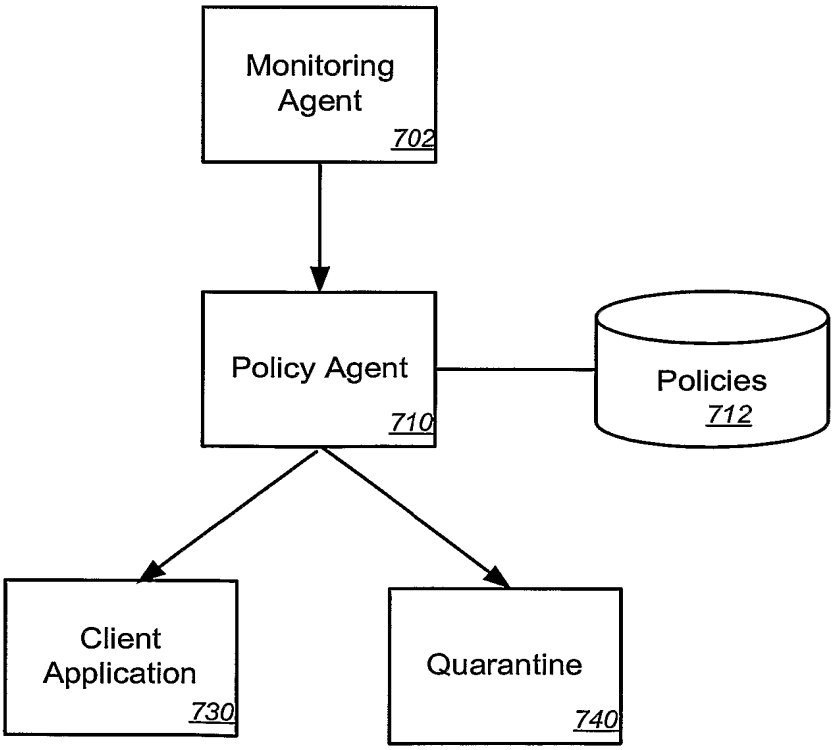
(74) Agents: **KING, Chad** et al.; Townsend and Townsend and Crew LLP, Two Embarcadero Center, Eighth Floor, San Francisco, California 94111-3834 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: IMPLEMENTING TRUST POLICIES



(57) Abstract: Embodiments of the present invention provide methods, systems, and software for implementing trust policies. Such policies may be implemented in a variety of ways, including at one or more border devices, client computers, etc. m accordance with various embodiments, a communication between a client computer (and/or application) and an online entity may be monitored and/or otherwise detected. The online entity may be identified, and/or one or more trust scores associated with the online entity may be obtained. Based on the trust scores, as well, perhaps as the nature of the communication, an action (such as allowing the communication, blocking the communication, quarantining the communication, warning a user, administrator, etc.) may be taken. In some cases, a trust policy may be consulted to determine what action should be taken with respect to a given communication.

WO 2006/094228 A2

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

IMPLEMENTING TRUST POLICIES

COPYRIGHT NOTICE

[0001] A portion of the disclosure of this patent document contains material that is subject to copyright protection. The copyright owner has no objection to the facsimile reproduction by anyone of the patent document or the patent disclosure as it appears in the Patent and Trademark Office patent file or records, but otherwise reserves all copyright rights whatsoever.

CROSS-REFERENCE TO RELATED APPLICATIONS

[0002] This application claims the benefit of the following provisional U.S. patent applications, of which the entire disclosure of each is incorporated herein by reference: provisional U.S. Pat. App. No. 60/658,124, entitled "Distribution of Trust Data," and filed March 2, 2005 by Shull et al.; provisional U.S. Pat. App. No. 60/658,087, entitled "Trust Evaluation Systems and Methods," and filed March 2, 2005 by Shull et al.; and provisional U.S. Pat. App. No. 60/658,281, entitled "Implementing Trust Policies," and filed March 2, 2005 by Shull et al.

[0003] This application is also related to the following applications, the entire disclosure of each of which is incorporated herein by reference: U.S. Pat. App. No. 11/339,985, entitled "Online Identity Tracking," and filed January 25, 2006 by Shull et al.; U.S. Pat. App. No. --/-----, entitled "Trust Evaluation Systems and Methods," and filed on a date even herewith by Shull et al. (attorney docket no. 040246-002410); and U.S. Pat. App. No. --/------, entitled "Distribution of Trust Data," and filed on a date even herewith by Shull et al. (attorney docket no. 040246-002310).

BACKGROUND

[0004] As ever more business is transacted online, the ability to evaluate online entities becomes increasingly important. For example, if a user desires to transact business

online with a particular entity, the user generally would like to be able to determine with a high degree of confidence that the entity actually is who it purports to be, and that the entity is trustworthy, at least for the purposes of the transaction. Various solutions have been proposed to provide some verifiable identification of entities, including without limitation the Domain Keys system proposed by Yahoo, Inc., the Sender Profile Form ("SPF") system, and the SenderID for Email scheme proposed by Microsoft, Inc. These systems all attempt to provide identity authentication, for example, by guaranteeing that an IP address or domain name attempting to transmit the email message, web page, or other data is the actual IP address or domain purporting to transmit the data, and not a spoofed IP address or domain name.

[0005] These solutions, however, fail to address a much larger issue. In many cases, the mere verification that a message originates from a particular domain provides little assurance of the character of the online entity. For certain well-known domains, such as <microsoft.com>, the domain name itself may provide a relatively reliable identification of the entity operating the domain, assuming no mistypings or unusual derivations containing some form of the name. For most domains and IP addresses, however, the domain name or source IP address cannot be considered, on its own, to provide reliable information on the trustworthiness of the underlying domain or IP address itself.

[0006] The well-known WHOIS protocol attempts to provide some identification of the entity owning a particular domain. Those skilled in the art will appreciate, however, that there is no authoritative or central WHOIS database that provides identification for every domain. Instead, various domain name registration entities (including without limitation registrars and registries) provide varying amounts of WHOIS registrant identity data, which means that there is no single, trusted or uniform source of domain name identity data. Moreover, many registrars and registries fail to follow any standard conventions for their WHOIS data structure, meaning that data from two different registrars or registries likely will be organized in different ways, making attempts to harmonize data from different databases difficult, to say the least. Further compounding the problem is that most WHOIS databases cannot be searched except by domain name, so that even if the owner of a given domain can be identified, it is difficult (if not impossible) to determine what other domains that owner owns, or even to determine whether the ownership information for a given domain is correct. Coupled with the reality that many domain owners provide mostly incorrect domain

information, this renders the WHOIS protocol virtually useless as a tool for verifying the identity of a domain owner.

[0007] The concept of a "reverse WHOIS" process has been proposed as one solution to this issue. Reverse WHOIS, which provides more sophisticated data-collection and searching methods for WHOIS information, is described in further detail in the following commonly-owned, co-pending applications, each of which is hereby incorporated by reference, and which are referred to collectively herein as the "Reverse WHOIS Applications": U.S. Pat. App. Nos. 11/009,524, 11/009,529, 11/ 009,530, and 11/009, 531 (all filed by Bura et al. on December 10, 2004). The concept of reverse WHOIS addresses some of the problems in identifying the owner of a domain. However, as with the WHOIS protocol, the reverse WHOIS protocol does not provide any indication of the trustworthiness of an online entity. Moreover, WHOIS data generally is not use programmatically.

[0008] Consider, for example, a situation in which an online fraud has been identified. Systems for identifying and responding to online fraud are described in detail in the following commonly-owned, co-pending applications, each of which is hereby incorporated by reference, and which are referred to collectively herein as the "Anti-Fraud Applications": U.S. Pat. App. No. 10/709,938 (filed by Shraim et al. on May 2, 2004); U.S. Pat. App. Nos. 10/996,566, 10/996,567, 10/996,568, 10/996,646, 10/996,990, 10/996,991, 10/996,993, and 10/997,626 (all filed by Shraim, Shull, et al. on November 23, 2004); and U.S. Pat. App. No. 11/237,642, filed by Shull et al. on September 27, 2005. In many cases, an IP address of a server engaged in online fraud may be available. However, there are currently no mechanisms to notify other entities that the domain name and/or IP address was associated with an online fraud.

[0009] Thus, mechanisms are needed to evaluate and provide an indication of the trustworthiness of online entities, including without limitation domain names and IP addresses, as well as the users and/or owners of those domain names and IP addresses.

BRIEF SUMMARY

[0010] Embodiments of the present invention provide methods, systems, and software for implementing trust policies. Such policies may be implemented in a variety of ways, including at one or more border devices, client computers, etc. In accordance with various

embodiments, a communication between a client computer (and/or application) and an online entity may be monitored and/or otherwise detected. The online entity may be identified, and/or one or more trust scores associated with the online entity may be obtained. Based on the trust scores, as well, perhaps as the nature of the communication, an action (such as allowing the communication, blocking the communication, quarantining the communication, warning a user, administrator, etc.) may be taken. In some cases, a trust policy may be consulted to determine what action should be taken with respect to a given communication.

[0011] Merely by way of example, one set of embodiments provides methods for evaluating a communication and/or implementing a trust policy. An exemplary method may comprise receiving, at a computer (which may be a client computer, a border device, etc.), a trust score score evaluating a trustworthiness of an online entity and/or taking an action with respect to a communication associated with the online entity.

[0012] The method may also further comprise consulting, e.g., with the computer, at least one trust policy. The action to take may be determined based at least in part on the reputation policy and the reputation score. In some cases, the action to take may be determined by comparing the reputation score to one or more values associated with the at least one reputation policy. The action may comprise, merely by way of example, blocking the communication, allowing the communication, quarantining the communication, transmitting a notification and/or a warning, etc.

[0013] In particular embodiments, the trust score may be one of a plurality of trust scores, including without limitation a trust score evaluating the likelihood of the online entity to engage in fraudulent behavior, a trust score evaluating the likelihood of the online entity to transmit unwanted communications, a trust score evaluating the likelihood of the online entity to engage in cybersquatting, and a trust score evaluating the likelihood of the online entity to engage in trademark abuse. The trust score, then may be a first trust score and/or may evaluating the trustworthiness of the online entity in a first category of behavior. The method may further comprise receiving a second trust score, which may evaluate the trustworthiness of the online entity in a second category of behavior.

[0014] Another set of embodiments provides systems, including without limitation systems implementing methods of the invention. Merely by way of example, a trust authentication system in accordance with embodiments of the invention may comprise a first

software component, which may be configured to monitor communications associated with one or more client applications for a communication with an online entity. The system may further comprise a second software component configured to obtain one or more trust scores associated with an online entity and/or a third software component, configured to take an action with respect to the communication with the online entity, perhaps based on at least one of the one or more trust scores associated with the online entity.

[0015] One or more of the components may execute on a client computer executing the client application(s), on a border device separate from the client computer, on a combination of the two, etc. One or more of the components may also be incorporated in and/or comprise a monitoring agent and/or a policy agent. Alternatively, one or more of the components may be incorporated in one or more of the client applications, in an application program separate from the client applications and/or within a software program (such as a toolbar, plug-in, extension, etc.) configured to operate in conjunction with at least one of the client applications.

[0016] The trust authentication system may also comprise a data store including one or more reputation policies. In these aspects, one or more of the software components may be configured to determine the action to take based on the one or more reputation policies. In other aspects, the reputation authentication system may further comprise a quarantine area to store quarantined communications, and/or the action may comprise quarantining the communication.

[0017] Another exemplary system may comprise a processor and/or instructions executable by a processor. The processor may be incorporated within a border device, a client computer, etc. In a set of embodiments, the instructions may be executable to monitor communications associated with one or more client applications for a communication with an online entity, obtain one or more trust scores associated with an online entity, and/or take an action with respect to the communication with the online entity, perhaps based on at least one of the one or more trust scores associated with the online entity.

[0018] In another set of embodiments, the instructions may be executable to monitor a plurality of communications associated with a plurality of client computers, identify an online entity (other than one of the client computers), which may be associated with one of the plurality of communications, obtain one or more trust scores associated with the online

entity and/or take an action with respect to the one of the plurality of communications, based on at least one of the one or more trust scores associated with the online entity.

[0019] Yet another set of embodiments provides software programs, including without limitation software programs for implementing methods of the invention. An exemplary software program, which may be embodied on at least one computer readable medium, may have instructions executable by a processor to receive a trust score evaluating a reputation of an online entity, and/or take an action (perhaps based on the trust score) with respect to a communication associated with the online entity.

[0020] A software program in accordance with another embodiment may comprise instructions executable to monitor communications associated with one or more client applications for a communication with an online entity, obtain one or more trust scores associated with an online entity, and/or take an action with respect to the communication with the online entity, perhaps based on at least one of the one or more trust scores associated with the online entity.

[0021] Another exemplary program may comprise instructions executable to monitor a plurality of communications associated with a plurality of client computers and/or dentify an online entity (other than one of the client computers), which may be associated with one of the plurality of communications. The instructions may be further executable to obtain one or more trust scores associated with the online entity and/or to take an action with respect to the one of the plurality of communications, perhaps based on at least one of the one or more trust scores associated with the online entity.

[0022] A further understanding of the nature and advantages of the present invention may be realized by reference to the remaining portions of the specification and the drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0023] Figure 1 illustrates exemplary sources of data that may be used by a trust evaluation system to determine the trustworthiness of online entities.

[0024] Figure 2 illustrates an exemplary block diagram of a system that may be used to provide trust data about online entities.

[0025] Figure 3 is a block diagram of a computer system upon which a trust evaluation system may be implemented.

[0026] Figure 4 is a flow diagram illustrating an exemplary method that may be used to evaluate the trustworthiness of an online entity.

[0027] Figure 5 illustrates a system that may be used to distribute trust data according to various embodiments.

[0028] Figure 6 illustrates a system that may be used to distribute trust data in accordance with various embodiments.

[0029] Figure 7 illustrates an exemplary system that may be used to apply trust polices to communications.

[0030] Figure 8 is a flow diagram illustrating an exemplary method that may be used to acquire trust data.

[0031] Figure 9 is a flow diagram illustrating an exemplary method that may be used to implement trust policies.

DETAILED DESCRIPTION

[0032] In the following description, for the purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the present invention. It will be apparent, however, to one skilled in the art that the present invention may be practiced without some of these specific details. In other instances, well-known structures and devices are shown in block diagram form.

[0033] Various embodiments of the invention provide the ability to calculate a trust score for an online entity based on the online entity's identification, relationships, history, and/or other information. Merely by way of example, data sets which may be acquired and used to evaluate an entity's trustworthiness may include, without limitation, WHOIS data, network registration data, UDRP data, DNS record data, hostname data, zone file data, fraud-related data, corporate records data, trademark registration data, hosting provider data, ISP and online provider acceptable use policy ("AUP") data, past security event data, case law data, and/or other primary and/or derived data related to the registration, background,

enabling services, and history of an entity on the Internet. The information used to evaluate an online entity may be gathered and correlated as described in U.S. Pat. App. No. 11/339,985, already incorporated by reference, as well as provisional U.S. Pat. App. No. 60/647109, filed January 25, 2005, entitled "Online Identity Tracking," the entire disclosure of which is hereby incorporated by reference. (Together, these two applications are referred to herein as the "Online Identity Tracking Application.")

[0034] The trust scores may be provided to third parties (such as users, administrators, ISPs, etc.) to allow those third parties to make determinations about the trustworthiness of an online entity. Based on such determinations, the third parties may choose to take specific actions with respect to communications and/or data received from the entity. In one set of embodiments, a structure similar to a DNS system, with caching servers, root servers (and/or core servers), and/or authoritative servers, may be provided to allow third parties to obtain trust scoring information about a particular entity.

[0035] An online entity may be a person and/or business (such as the owner of a domain, the operator of a server, etc.), a domain name, a hostname, an IP address (and/or network block), a computer (such as a server) and/or any other person or thing that maintains an online presence and therefore is capable of being identified. Particular embodiments, therefore, may calculate trust scores based on information stored in one or more databases (which may be global and/or searchable) that can be used to provide records, experience and/or other information about the ownership, relationship, historical, and/or behavioral attributes of entities on the Internet, including domain names, IP addresses, registrars, registries and ISPs. These databases may be used to determine associations between online entities and illicit activities, including without limitation phishing scams, trademark infringement, fraudulent sales and/or solicitations, misappropriation of identities and/or brand names, unwanted spam and/or pop-up windows, viruses, malicious code, spyware, trojans, and/or other security threats, and/or other illegitimate activities. In accordance with some embodiments, trust scores may be used to predict the trustworthiness of an online entity.

[0036] Particular embodiments further provide the ability for trust database(s) (also referred to herein and in the Online Identity Tracking Application as reputation databases and/or reputational databases) to interact functionally and/or to be used in conjunction with other authentication schemes, including without limitation DNS-based schemes, such as SPF, Domain Keys, etc., to provide authentication of the domain name and/or IP address as well as

providing a score to inform a user, administrator and/or application of the trustworthiness of the entity associated with the domain name or IP address. The identifying information and/or aggregate history of the domain name and/or IP address may also be analyzed and/or assigned a probability score indicating the probability that the entity is trustworthy. As used in this context, the term "trustworthy" means that the entity is engaged in legitimate online activity, as opposed to unsafe, dangerous, unwanted and/or otherwise illegitimate activities (which can include a variety of online activities, such as phishing and/or other types of fraud and/or abuse, cybersquatting, legal and/or illegal pornography, transmitting spam, pop-up messages and/or any other types of unwanted communications, viruses, malicious code, spyware, trojans, and/or other security threats). In accordance with various embodiments and implementations, any of a variety of questionable activities may be considered illegitimate and therefore might render an entity performing such activities as untrustworthy. The term "reputation" is sometimes used herein to indicate an entity's reputation (as determined by embodiments of the invention) as being relatively trustworthy or untrustworthy.

[0037] It should be noted that, while existing anti-spam systems purport to implement "reputation databases," those databases merely track the senders of spam and allow for the compilation of complaints from users about those senders. Embodiments of the current invention provide a much more robust framework for evaluating the trustworthiness (perhaps across a variety of characteristics and/or categories of activity) of any particular entity, rather than merely tracking purveyors of spam.

[0038] In an aspect of the invention, some embodiments can be considered to associate or bind a trust score to an authenticated source name (which could be a domain name, personal name, corporate name, IP address, etc.). If the source name is authenticated (using, for example, a standard authentication scheme, such as SPF, SenderID for Email, DomainKeys, etc., and/or authentication by the trust provider or a third party, using, for example, an identity tracking system and/or the like), the trust score is likely to be relatively more reliable and/or valuable, since the combination of authentication and trust score ensures that a user knows first that an entity is who that entity purports to be and second that the entity is trustworthy. Nonetheless, trust scores may also be provided for unauthenticated entities (and, as described herein, the fact that an entity has not been authenticated may be a factor to be considered in determining the trust score). In some embodiments, neither the sender of the communication nor the recipient need know either other (or even actively

participate in the trust evaluation process) in order for trust evaluation services to be provided.

[0039] Such a score might be made available to users (and/or others, such as administrators and/or applications) via a secure and/or authenticated communication. The score might be matched with a domain name and/or IP address authenticated via one of the authentication schemes mentioned above and/or any encryption, authentication, non-repudiation and/or other security schemes. The user (or other) would be able to see and/or use the score, which may be provided by an authoritative server (such as a trust evaluation system, described below), one or more root and/or caching servers (which may include copies of one or more score databases, as described below, and/or pointers to an authoritative source for scores), and/or the like. In a particular set of embodiments, score information may be provided by enhancements to the current domain name system ("DNS") and/or various certification systems and/or by a hierarchical system with a structure similar to the DNS, and use the transmitted data accordingly.

[0040] In a set of embodiments, the trust score indicates the overall trustworthiness of the entity and/or the likelihood that the entity is a source of fraud, abuse, unwanted traffic and/or content (such as spam, unwanted pop-up windows, etc.), viruses, etc. and/or the entity's trustworthiness in general and/or for specific situations, such as commercial transactions, etc. Trust score(s) can also be used as input to inform a broader policy manager (which might operate on an ISP-wide and/or enterprise-wide level, and/or at the individual computer, operating system, application and/or user level for example), which dictates how specific traffic should be handled, based on the score of an online entity originating that traffic and/or the score of the intended recipient of the traffic. Merely by way of example, based on the score associated with a given communication (such as an email message, HTTP transmission, etc.), that communication might be allowed, blocked, quarantined, tracked, and/or recorded (e.g., for further analysis), and/or a user and/or administrator might be warned about the communication. Other security and/or business policies could be implemented as well. For instance, this exemplary model may provide a simple, and therefore fast way to handle communications with various entities. It may be used across multiple categories of trust scores, and/or it may be expanded, restricted and/or modified to accommodate other requirements, such as for a richer set of handling options. Various categories in which scores may be accorded different handling options might include any

types of communications that a user might want to treat in various ways, including by way of example, pornography, spam, phishing attacks, etc. For instance, a given user might not mind receiving spam but might be very wary of phishing scams, so the user might configure a trust application to allow relatively free communications with entities having a relatively poor reputation with respect to sending spam but to be very restrictive on communications from (or to) entities with a reputation of being associated (even loosely) with phishing scams. Hence, polices can be tuned to account for types of traffic and/or to filter based on personal preferences.

[0041] Such policies may be implemented in a variety of ways. Merely by way of example, a border device (such as a firewall, proxy, router, etc.) that serves as a gateway to an enterprise, etc. may be configured to obtain a score for each incoming (and/or outgoing) communication, and based on that score, take an appropriate action (such as one of the actions described above). As another example, client software on a user's computer may be configured to obtain a score for each communication and act accordingly. For instance, a web browser, application and/or operating system might be configured (via native configuration options and/or via a toolbar, plug-in, extension, etc.) to obtain a score (e.g., from a server, etc.) for each web page downloaded (and/or, more specifically, for the entity transmitting the web page). If that score, for instance, indicated that the web page was likely to be a phishing attempt or evidence other risky or unwanted characteristics, the browser could warn the user of that fact and/or could refused to load the page (perhaps with a suitable warning to the user), and/or to take other appropriate action(s). Embodiments of the invention may be configured to provide multiple and/or parallel alert levels or types, depending on various scores accorded the entity associated with a given communication. Other embodiments might also provide active selection, quarantine, filtering and/or dropping of various communications.

[0042] An email client application might operate similarly with respect to email. For example, the email client may use one or more trust scores to determine a probability that an email contains a virus, is associated with a fraudulent activity, is associated with a phishing attempt, and/or is likely to be unwanted traffic (spam, pop-ups, pornography, etc.). Accordingly, based on the trust score(s), the email client may quarantine the message, block the message, warn the user, allow the message to pass or take other appropriate action.

[0043] Trust score(s) may be analogized roughly to a credit score. Based on a history (generally of multiple inputs and/or security events) and/or with other ascertained identification information, score(s) may be derived and/or used in real-time, near-real-time and/or asynchronous transaction processing. As with credit card scores, trust score(s) may change over time based on updated information. While various embodiments may provide a variety of evaluation information to users (and/or others), a simple scoring system (e.g., 1-5, as described elsewhere herein) allows the system to be both fast and extensible (since multiple scores, based on various characteristics and/or categories of behavior, such as spam, fraud, phishing, pornography, etc., may be accorded a single entity).

[0044] Thus, embodiments of the invention provide mechanisms to evaluate and provide indications of the trustworthiness (reputation) of, and/or predetermined interest in, online entitles.

[0045] Figure 1 illustrates exemplary sources of data that may be used by a trust evaluation system to determine the trust scores of online entities. Trust evaluation system 102 may comprise one or more computers (including, merely by way of example, personal computers, servers, minicomputers, mainframe computers, etc.) running one or more appropriate operating systems (such as any appropriate variety of Microsoft Windows; UNIX or UNIX-like operating systems, such as OpenBSD, Linux, etc.; mainframe operating systems, such as OS390, etc.), along with application software configured to perform methods and/or procedures in accordance with embodiments of the invention. In particular embodiments, trust evaluation system 102 may comprise, be incorporated in and/or operate in conjunction with any of the systems (and/or elements thereof) described in the Anti-Fraud Applications and/or the Online Identity Tracking Application.

[0046] Trust evaluation system 102 may be communicatively coupled with any number of different data sources 131-165 and/or other computers (not illustrated) via one or more networks 110. By way of example, network(s) 110 may include the Internet or other public area network(s) or private network(s). Other types of networks capable of supporting data communications between computers (such as cellular and/or wireless networks supporting Internet traffic between phones and other wireless devices) will also suffice.

[0047] Data sources 131-165 may contain information used by trust evaluation system 102 to evaluate and calculate trust score(s) for online entities. Various data sources,

and methods and systems that may be used to gather and correlate data from data sources are described in further detail in the Online Identity Tracking Application. In some embodiments, the gathering and/or correlation of data from data sources 131-165 may be alternatively or additionally be performed by systems other than trust evaluation system 102. Thus, trust evaluation system 102 may obtain correlated data from one or more intermediary systems (not shown) interspersed between data source 131-165 and trust evaluation system 102.

[0048] Data sources used by trust evaluation system to evaluate and determine trust score(s) for online entities may include, without limitation, sources 131-136 of registration data, sources 141-146 of background data, sources 151-159 of harvested data, and/or sources 161-165 from and/or about enabling parties. The information from data sources 131-165 may be collected using any suitable operation designed to obtain data.

[0049] Registration data sources may include one or more WHOIS databases 131. Another type of registration data source may be network registration databases 132, such as databases maintained by ARIN, APNIC, LACNIC, RIPE and/or other entities responsible for allocating and/or maintaining records of IP addresses and/or networks. Other sources of registration data may include DNS data 133 (e.g., DNS databases or tables which may contain information related to DNS addressing of various hosts and/or networks), name servers 134, Internet root servers and/or systems that feed updates to root servers (not shown in Fig. 1), certificate authorities 135 (responsible for issuing and managing security credentials and/or public keys), or other public directory data sources 136. Data used by trust evaluation system 102 may also be obtained from other types of registration data sources.

[0050] Background data may be obtained from background data sources, such as data sources 141-146. UDRP data sources 141 may contain data related to UDRP complaints filed against online entities. Trademark data sources 142 may provide information relating to ownership of registered and/or unregistered trademarks. Corporate record data sources 143 may provide information related to the identities and/or ownership of various business entities, including but not limited to corporations. Other sources of background data may include credit history data 144, judicial records 145, other public record sources 146 (e.g., property records, telephone directories, voting records, tax records, etc.), and/or any other type of data source that may provide background information on an online entity.

[0051] Data may also be compiled and/or derived through monitoring, crawling, and/or anti-fraud operations. Exemplary harvesting operations are described in the Anti-Fraud Applications previously incorporated by reference, although any other harvesting technique may also be used to obtain the data. Merely by way of example, harvested data may include zone file updates 151 which can comprise comparisons or "diff" files of changes from one version of a zone file to the next. This may allow for the relatively expeditious ascertainment of new and/or modified domain registrations. Other exemplary sources of harvested data may include brand abuse data 152, fraud detection data 153 (which may include results of fraud detection/prevention operations and/or investigations), graphic detection data 154, geographical location data 155 (which may indicate geographical regions known to originate high percentages of fraudulent/illicit activities or other type of geographical information), ISP feeds 156 (which can comprise one or more email feeds of potential spam and/or phish messages), planted feed data 157 (feeds and/or results of planting operations), honeypots 158, and/or decrypted detection data 159 (detecting decryption operations). Further details and examples of ISP feeds 156, planted feeds 157 and honeypots 158 are described in the Anti-Fraud Applications previously incorporated by reference.

[0052] It should be appreciated that other types of harvested data may also be used by trust evaluation system 102 to determine reputations of online entities. Merely by way of example, U.S. Pat. App. No. 11/237,642. already incorporated by references, describes systems that can be used to provide harvested data for determining reputations of online entities. Further sources of data can include feeds from search engines, security providers and/or ISPs, rating services (including whitelists, blacklists, etc.) and/or the like.

[0053] Data from and/or about enabling parties may also be used by trust evaluation system 102. An "enabling party," as that term is used herein, can be any party that provides services facilitating an entity's presence on the Internet. Examples of enabling parties can include, without limitation, registrars 161 and/or registries 162, ISPs 163, hosting providers 164, DNS providers 165, and/or the like. Data about and/or from these parties can include data compiled and/or maintained by these providers about their customers, data about the providers themselves (including, merely by way of example, identifiers such as IP addresses, domains, network blocks, addresses, locations, legal jurisdictions, acceptable use policies, ICANN and/or other regulatory compliance policies and/or practices, data integrity, practices of promoting, selling to and/or shielding known participants in illegitimate activities, etc. that

may identify a provider), trends and/or amenability of a given provider to facilitate illicit activity, historical behavior of customers of a given provider, etc.

[0054] As previously described, any suitable technique may be used to gather data from data sources 131-165. Once the data is gathered it may be cross-indexed and/or cross-referenced based on matching or similar information. Merely by way of example, if a harvested WHOIS record contains information for a particular domain, and a harvested DNS record provides name server information for a host in that particular domain, the information in the DNS record may be cross-indexed and/or cross-referenced against that WHOIS record. Data may also be grouped. If for instances, an identified individual owns other domains, information about those domains may be associated with each other and/or grouped with other cross-indexed information. Further details about data correlation may be found in the Online Identity Tracking Application previously incorporated by reference.

[0055] The correlation of data from a variety of data sources may provide predictive functionality. For example, if a particular individual is associated with a known phishing scam, any other IP addresses, domain names, etc. associated with that individual (through, for example, a cross-indexing operation), may be assumed to be relatively more likely to be involved in phishing scams as well (and/or, as described below, may be scored and/or added to a greylist as an associate of a known participant in illegitimate activity). Through these cross-indexing associations, trend information may be revealed as well. Merely by way of example, an analysis of associations may reveal that a particular ISP, domain name registry and/or name server is relatively more likely to be a provider for phishing operations. Other domains and/or IP addresses associated (again, through the cross-indexing procedures and/or through other procedures) with that provider may then be relatively more likely to be involved in illicit activities. Hence, it may be appropriate to block a set of domains and/or a range of IP addresses, if the data reveals a pattern of abuse relating to parties associated with such domains and/or addresses.

[0056] In this way, trust evaluation system 102 may use correlated data gathered from data sources, such as data sources 131-165, to develop a trust database. For any online entity, for example, an analysis of some or all cross-indexed and/or associated data may allow a relatively confident determination of whether that individual, who may attempt to deceive a user (or another), is in fact involved in illicit and/or unwanted online activity. Merely by way of example, if a domain owner uses the services of a registry and/or ISP known to be friendly

to phishers, pornographers, etc., it may be relatively more likely that a web site hosted on that domain may be a phish site, pornography site, etc. These relationships can easily be ascertained through the cross-indexing and cross-reference relationships supported by embodiments of the invention.

[0057] Trust evaluation system 102 may also provide a historical view of an entity's activities. Merely by way of example, if it is discovered that a given entity is engaging in an illicit activity, such as phishing, a record of the activity may be made with respect to that entity. Further, a record may be made with respect to each of the enabling parties associated with that entity, thereby tagging and/or labeling such enablers as being relatively more likely to facilitate illicit activities. Each time an enabling party is discovered to be a facilitator of such activity (and/or refuses to take corrective action when notified of such activity), a trust score may be adjusted. Trust score(s) may allow interested parties to determine quickly whether a given enabling party is relatively more or less likely to act as a facilitator of illicit activity, which can provide insight into the likelihood of a entity associated with such an enabling party to be engaged in an illicit activity and/or can allow the preparation of a complaint against an enabling party, etc.

[0058] As described in further detail below, embodiments of the invention may be used to provide a security and/or authentication service to users, companies, ISPs, etc. In such embodiments, for example, a trust provider may provide and/or maintain trust (reputational) and/or scoring databases for use by its customers. (A trust provider may be any entity that provides entity verification and/or evaluation services, including the scoring services discussed herein. A trust provider may also maintain and/or operate a trust evaluation system and/or may ensure the integrity of any replicated and/or cached trust or scoring databases, as described in detail below.) Such databases may be consulted to determine the relative reliability of various online entities in adhering to determined characteristics. In a particular embodiment, the scores may be, as noted above, analogous to credit scores, such that each entity is accorded a score based on its identifying information, relationship information, and history. Such scores may be dynamic, similar to credit scores, such that an entity's score may change over time, based on that entity's relationships, activities, etc. Merely by way of example, a scoring system from 1 to 5 may be implemented. A score of 1 may indicate the online entity has been verified and/or certified reliable by a provider of the trust evaluation system, such as through a certification process. A score of 2

may indicate that the entity is relatively likely to be reputable (that is, to be engaged only in legitimate activities), while a score of 3 may indicate that the identification and/or reputation of an entity is doubtful and/or cannot be authenticated, and scores of 4 or 5 indicate that the entity is known to be disreputable (e.g., engage in and/or facilitate illicit activity).

[0059] This exemplary scoring scheme is designed to be extensible, in that a plurality of scores may be accorded to any given entity, based perhaps on various characteristics and/or categories of activities. Merely by way of example, an entity may be accorded a number of scores based on that entity's likelihood of being involved in phishing and/or other fraudulent activities, brand abuse, pornography, e-commerce, online transactions, consumer targeting, preferred programs, service expedition, etc. (It may be noted from the above list that not all activities need to be illegitimate activities. Merely by way of example, a score indicating that an entity is likely to be engaged in e-commerce may allow a user to infer that a transaction with that entity is relatively more likely to be a legitimate transaction and/or may be used by a security system on a client and/or a border device (including those described below, for example) to make a determination that a transaction with such an entity is an allowable communication.

[0060] It should be noted that, while the above scoring scheme is used throughout several examples herein for illustrative purposes, the scheme is merely exemplary in nature, and that the procedure for evaluating and/or entities is discretionary.

[0061] In a set of embodiments, trust evaluation system 102 may provide trust score(s) as a relatively objective determination of the trustworthiness of an entity. A user, company, ISP, etc. may make its own determination of how to treat communications, data, etc. from an entity, based upon that entity's score. Merely by way of example, a company and/or ISP might configure its mail server to check the score of each entity from whom the server receives mail, and to take a specific action (e.g., forward the mail to its intended recipient, attach a warning to the mail, quarantine the mail, discard the mail, etc.) for each message, based on the score of the sending entity. As another example, a web browser might be configured to check the score of web site when the user attempts to access the site and take a specific action (e.g., block access to the site, warn the user, allow access to the site, etc.), based on the score of the web site (and/or an entity associated with the web site).

[0062] Trust evaluation system 102 may distribute trust score(s) using an enhancement of the current DNS and/or certification systems and/or a structure similar to the DNS structure. For instance, in some embodiments, trust evaluation system 102 may provide a root (authoritative) scoring server, and various entities (ISPs, etc.) might provide caching scoring servers. If a score lookup is needed, an assigned caching server might be consulted, and if that caching server has incomplete and/or expired scoring information, a root server may be consulted. Root servers might ultimately obtain scoring information from trust evaluation system 102, which may act as the authoritative server for the trust scores. In particular embodiments, however, unlike DNS, trust evaluation system 102 (and/or another trusted source), would have control over the dissemination of scoring information, such that the scoring servers could not be modified by third parties, and scoring information could not be compromised, either in transit or at the caching servers. Secure and/or encrypted transmission, authentication, non-repudiation and/or storage protocols thus might be implemented to ensure data integrity.

[0063] Figure 2 illustrates an exemplary embodiment of a trust evaluation system 200. Trust evaluation system 200 may include one or more data stores 202. Data stores 202 may be used to store data gathered from a plurality of data sources (e.g., any of the data sources illustrated in Figure 1) which has been cross-indexed and/or cross-referenced to correlate the data from the different sources. The gathering and/or correlation of the data may be performed by trust evaluation system 200 or other system.

[0064] Trust evaluation system 200 may further include a scoring engine 210 communicatively coupled with data store(s) 202. A communicative coupling is any type of coupling that allows communication between components (e.g., bus, external network connection, etc.). Thus, it should be appreciated that components which are communicatively coupled may reside on the same or different physical device(s).

[0065] Scoring engine 210 may calculate one or more trust score(s) for each of a plurality of online entities based on data 202 correlated to the respective online entity. Scoring engine 210 may also or alternatively calculate one or more derived score(s) 231-238 to evaluate a factor of data correlated to online entities. The derived score(s) 231-238 may optionally be used by scoring engine 210 to calculate trust score(s). As the data in data store(s) 202 may constantly or periodically be updated, scoring engine 210 may update trust

score(s) and/or derived score(s) 231-238 on a periodic basis and/or upon detection of a specific event (e.g., an identification of a new fraudulent entity).

[0066] Derived score(s) 231-238 calculated by scoring engine 210 may be stored in one or more data stores (e.g., one or more relational databases, XML file(s), internal software list(s), or other suitable data structure). Alternatively, scoring engine 210 may dynamically calculate derived score(s) 231-238 as needed without storing calculated derived score(s) 231-238. In still further embodiments, scoring engine 210 may not calculate derived scores 231-238 at all.

[0067] One example of a type of derived score that may be calculated by scoring engine 210 is a consistency score 231. A consistency score for a particular online entity may evaluate a consistency factor of data associated with the online entity. For example, if the data correlated to an online entity indicates that all IP addresses associated with the online entity are on the same network, the online entity may receive a relatively high consistency score. Similarly, if IP addresses associated with the online entity are on a number of different networks, the online entity may receive a relatively low consistency score. As another example, the calculation of a consistency score may also or alternatively evaluate whether a quality of information associated with the online entity is consistent (e.g., WHOIS records are of a consistent quality and/or contain consistent information). Other information may also be evaluated by scoring engine 202 to determine consistency scores 231 for online entities.

[0068] Another type of derived score that that may be calculated by scoring engine for an online entity is a secure infrastructure score 232. Secure infrastructure scores 232 may be used to evaluate and score an online entity's use of security features, such as certificates. Other exemplary types of derived scores include trusted record scores 233 (evaluating and scoring entities based on the respective online entity's history with trusted data sources), change scores 234 (evaluating and scoring the frequency with which an online entity changes domain registrations), whitelist and/or blacklist scores 235 (evaluating and scoring an online entity's suitability for a whitelist (very high repute) or blacklist (disreputable)), history scores 236 (evaluating historical data to determine an entity's online history, lack of history and/or a quality of that history), portfolio scores 237 (evaluating and scoring the online entity based on whether an online portfolio (domain names owned, activities performed, etc.) associated with the online entity is compatible (makes sense) with the nature and character of the online entity), and/or any other type of derived score which evaluates a factor of correlated data

associated with an online entity. Other scores can include application scores and virus scores, which can evaluate the trustworthiness of particular applications and/or malicious code (such that, when a user attempts to install such applications and/or code, the scores can be used to either advise the user on whether the application should be installed and/or make a determination (e.g., at an operating system and/or domain policy level) whether to allow or prohibit such installation).

[0069] Derived score(s) 231-238 may be calculated using any suitable data from data store(s) 202 or other derived scores for the particular derived score being calculated. Merely by way example, a portfolio score for an online entity, such as a corporation or entity associated with a corporation (e.g., IP address), may include factors such as a size of the corporation (which may be determined from data derived from corporate records) and/or a number of IP addresses owned by the corporation (obtained from correlated WHOIS data, DNS data, etc.). As another example, a calculation of a secure infrastructure score may include a factor counting a number of certificates associated with an online entity, number of unsecured servers associated with the entity, etc.. It should be appreciated that numerous other types of calculations are possible and that embodiments may use a variety of techniques to calculate derived scores based on types of data available in the data store 202 and/or varying requirements for the derived scores being calculated.

[0070] Scoring engine 210 may use derived scores 231-238 and/or correlated data obtained from data store(s) 202 to calculate one or more trust scores for an online entity. Any type of statistical analysis (e.g., direct, Bayesian, fuzzy, heuristic, and/or other types of statistical relationships) may be used by scoring engine 210 to calculate trust score(s). Trust score(s) may be dynamic, such that an entity's score may change over time based on that entity's relationships, activities, or other factors. As with credit card scores(s), competing trust evaluation systems 200 may vary on the factors and algorithms used to calculate trust score(s).

[0071] Trust score(s) that are calculated for a particular type of entity may use any type of data correlated with the online entity as factors in the calculation. Merely by way of example, a trust score for an IP address may include factors related to the individual or corporate entity owning the IP address, such as information obtained from corporate records, judicial records, or other type of data source. These relationships may be discovered and/or analyzed by an identity tracking system, such as the systems described in the Online Identity

Tracking Application, to name but a few examples. In further aspects, scoring engine 210 may use a trust score for a first online entity as a factor in calculating a trust score for a second online entity associated with the first online entity. Thus, if an IP address has a poor trust score (as derived by embodiments of the invention), other IP addresses owned by the same entity may receive a poor or doubtful trust score by association (especially if the owner of the addresses is an authenticated entity). Third party ratings for various characteristics being scored might also be consulted in determining scores.

[0072] Other factors may also be used in the calculation of trust score(s). By way of example, trust evaluation system 102 may include a feedback loop that allows entities to communicate feedback on trust scores. Received feedback may be included in subsequent calculations of the trust score for the online entity associated with the feedback. Safeguards may be provided to ensure that feedback communications can not unduly sway trust scores. Feedback may originate from customers of the provider of the trust evaluation system 102 or others, based on the experiences of the customers and/or the customers'/entities' own scoring evaluation(s). Feedback from systems such as those described in U.S. Pat. App. No. 11/237,642, already incorporated by reference, may also be used.

[0073] In one set of embodiments, scoring engine 210 may calculate overall trust scores using a scoring system from 1 to 5. Scores of 1 or 2 may indicate that the entity is relatively likely to be reputable (that is, to be engaged only in legitimate activities), while a score of 3 may indicate that the identification and/or reputation of an entity is doubtful and/or cannot be authenticated, and scores of 4 or 5 indicate that the entity is known to be disreputable (engage in and/or facilitate illicit activity). Other scoring mechanisms may also be used to calculate an online entity's overall reputation and/or trustworthiness.

[0074] Trust score(s) 210 may be stored in a trust data store 220, which may be made available and distributed by any appropriate mechanism, including without limitation those described below. Trust scores may each be associated with an identifier (e.g., domain name, corporation name, personal name, IP address, etc.) identifying the online entity associated with the respective score. In some embodiments, scoring engine 210 may calculate overall trust score(s) for IP addresses and/or domain names and/or may associate an entity's trust score (e.g., owner of IP address/domain) with IP addresses correlated to the entity as well as, optionally, associated enabling parties. This may provide for the ability of trust scores to be easily and rapidly distributed. Optionally, IP addresses and/or domain names (or other type

of online entity) with little or no available information (and/or that cannot be authenticated) may be assigned an initial score by scoring engine 210. In some aspects, a relatively neutral or uncertain score may be assigned such entities. In other cases, unknown entities may be assumed reputable (or disreputable). In a set of embodiments, the quality of the score might be quantified. Merely by way of example, a score that is the result of multiple independent scoring processes might be considered more reliable than a score that is provided by a single third party and has not been verified as accurate.

[0075] In some aspects, scoring engine 210 may also calculate specific types of trust scores. Merely by way of example, with respect to a particular online entity, scoring engine 210 may calculate a fraud trust score that evaluates the entity's reputation for and/or likelihood to be engaged in fraudulent activity. As another example, scoring engine 210 may calculate a virus trust score evaluating an entity's reputation for and/or likelihood to be engaged in perpetrating and/or perpetuating viruses. A third example is an unwanted traffic score evaluating the entity's reputation for and/or likelihood to be engaged in distributing unwanted traffic (spam, pornography, pop-up messages, malicious code, etc.). A fourth example is a cybersquatting trust score evaluating the entity's reputation of and/or likelihood of being a cybersquatter. Other specific types of trust scores related to a particular type of behavior may also be calculated by scoring engine 210. Thus, an online entity may have a plurality of associated trust scores, some or all of which may be stored in data store 220 and/or a plurality of data stores.

[0076] Figure 3 illustrates one embodiment of a computer system 300 upon which a trust evaluation system (or components of a trust evaluation system) may be implemented. The computer system 300 is shown comprising hardware elements that may be electrically coupled via a bus 355. The hardware elements may include one or more central processing units (CPUs) 305; one or more input devices 310 (e.g., a mouse, a keyboard, etc.); and one or more output devices 315 (e.g., a display device, a printer, etc.). The computer system 300 may also include one or more storage device 320. By way of example, storage device(s) 320 may be disk drives, optical storage devices, solid-state storage device such as a random access memory ("RAM") and/or a read-only memory ("ROM"), which can be programmable, flash-updateable and/or the like.

[0077] The computer system 300 may additionally include a computer-readable storage media reader 325; a communications system 330 (e.g., a modem, a network card

(wireless or wired), an infra-red communication device, etc.); and working memory 340, which may include RAM and ROM devices as described above. In some embodiments, the computer system 300 may also include a processing acceleration unit 335 , which can include a DSP, a special-purpose processor and/or the like

[0078] The computer-readable storage media reader 325 can further be connected to a computer-readable storage medium, together (and, optionally, in combination with storage device(s) 320) comprehensively representing remote, local, fixed, and/or removable storage devices plus storage media for temporarily and/or more permanently containing computer-readable information. The communications system 330 may permit data to be exchanged with a network and/or any other computer.

[0079] The computer system 300 may also comprise software elements, shown as being currently located within a working memory 340, including an operating system 345 and/or other code 350, such as application program(s). Application program(s) may implement a trust evaluation system. It should be appreciate that alternate embodiments of a computer system 300 may have numerous variations from that described above. For example, customized hardware might also be used and/or particular elements might be implemented in hardware, software (including portable software, such as applets), or both. Further, connection to other computing devices such as network input/output devices may be employed.

[0080] Figure 4 illustrates an exemplary method that may be used by a trust evaluation system to evaluate a the trustworthiness of an online entity. Data associated with an online entity may be retrieved 402 from one or more data sources. The data may have been compiled from a plurality of data sources and/or correlated as described above.

[0081] Optionally, one or more derived scores for the online entity may be calculated 410, perhaps based on the correlated data. Each calculated derived score may evaluate a factor of the data associated with the online entity. Derived score(s) calculated 410 for the online entity may comprise one or more of a consistency score 411, a trusted record score 412, a whitelist score 413, a blacklist score 414, a portfolio score 415, a secure infrastructure score 416, a change score 417, a history score 418, and/or other derived scores (including without limitation a compliance score, a data integrity score, an association score, a score related to the entity's facilitation of the illegitimate activities of others, etc.). In some

embodiments, derived score(s) may be stored 420 for future use or reference. Further details about the particular types of derived scores mentioned by way of example are described above with reference to Figure 2.

[0082] An overall trust score for the online entity may be calculated 422 based on the correlated data associated with the online entity. In some aspects, calculating 422 the overall trust score may include the use of calculated derived scores (such as the scores 411-419 discussed above) which evaluate one or more factors of the correlated data. In some embodiments, calculating 422 the overall score may comprise assigning the online entity a score from 1 to 5, with 1 indicating the entity is relatively likely to be reputable and 5 indicating the entity is relatively likely to be disreputable. Other scoring mechanisms may also be used.

[0083] In some aspects, one or more additional trust score(s) may also be calculated 424 for the entity. Additional trust score(s) may include a fraud trust score, a virus trust score, an unwanted traffic trust score, a cybersquatting trust score, examples of which are described above, and/or other specific types of trust scores. Some embodiments may not include the calculation 424 of additional trust scores.

[0084] The overall trust score and/or additional trust score(s) may be stored 426 in one or more trust data stores, perhaps along with an identifier identifying the online entity. The scores and/or other reputational information may then be made available to clients of trust evaluation system 200 and/or may be distributed, e.g. as described below.

[0085] Figure 5 illustrates an exemplary system that may be used to distribute and/or acquire trust data. The system includes a client application 502 communicatively coupled with monitoring agent 510. Client application 502 may be any type of application engaging in communications with online entities 520. By way of example, client application 502 may be a email application or a web browser application

[0086] Communications transmitted from and/or received by client application 502 may be monitored by monitoring agent 510 or other component. Upon detection of a communication associated with an online entity (e.g., request for data from the online entity or inbound communication received from the online entity), monitoring agent 510 may obtain one or more trust score(s) associated with the online entity. In some embodiments, monitoring agent 510 may first determine if the trust score(s) for the online entity are cached

in a local trust cache 512. If not, monitoring agent 510 may issue a request to a trust score server 530 for the online entity's trust score(s). Further details of a process that may be used to acquire trust data are described below with reference to Figure 8.

[0087] In some embodiments, monitoring agent 510 may reside on a border device (such as a firewall, proxy, router, etc.) that serves as a gateway to a network. In other embodiments, monitoring agent 510 may reside on the same computer as client application 502 or different computer. It should be appreciated that monitoring agent 510 may be a component of an operating system and/or a larger application (e.g., a native component, plug-in component, and/or a toolbar of a web-browser application, an email application, a gateway/firewall application, an anti-virus application, an anti-fraud application, a security suite, etc.) or may be a standalone application.

[0088] As previously described, trust evaluation system 540 may evaluate and create trust score(s) for online entities based on correlated data compiled from one or more sources. Trust evaluation system 540 may distribute trust score(s) using a structure similar to DNS. Thus, trust evaluation system 540 may maintain one or more authoritative trust data stores(s). Trust evaluation system 540, or authoritative database(s) component(s) of trust evaluation system 540, may be in communication with one or more trust score servers 530, which cache 532 at least a subset of the trust score(s).

[0089] In various embodiments, some of the trust score server(s) 530 may be root servers and/or core servers that receive trust scores from trust evaluation system 540. Trust scores may be transmitted to root servers using any or both of a pull mechanism (upon request of root server) or a push mechanism (at the initiation of trust evaluation system 540). Root servers may then be responsible for providing trust scores to a set of trust score servers 530 at a lower hierarchical level in the distribution chain. A different type of organizational structure of trust score server(s) 530 may also be used. In particular embodiments, for example, a system similar to DNS might be used, such that root (and/or core) servers contain pointers to one or more authoritative servers that have score information for requested entities. In other embodiments, however, each root (and/or core) server may have a complete and/or partial copy of one or more score databases, and may provide scores upon request (e.g., if a caching server and/or local cache does not have a score).

[0090] In a particular set of embodiments, there may be a plurality of authoritative trust servers (which may be trust evaluation systems, as described above, and/or servers in communication with a trust evaluation system). The authoritative trust servers, as noted above, serve as an authoritative source for trust scores; in some embodiments, each authoritative trust server may be responsible for a subset of trust scores. Merely by way of example, trust scores may be grouped by type of score (e.g., one authoritative trust server may be responsible for a set of trust scores related to one characteristic and/or category of behavior or interest, such as phishing, while another authoritative trust server is responsible for a set of trust scores related to another characteristic and/or category of behavior or interest, such as pornography). Characteristics of interest, for example, can be used for specific filtering criteria and/or selective searching of entities.

[0091] Alternatively and/or in addition, different authoritative servers may be used to implement different scoring criteria and/or scales, depending on the implementation. Thus, for example, a first authoritative server may have scores on a scale of 1-5 for a plurality of entities, while a second authoritative server may have scores on a scale of 1-25 for the same plurality of entities. A third authoritative server may simply contain blacklists, whitelists, and/or greylists of entities (which lists may be compiled based on trust scores).

[0092] In further embodiments, each of a plurality of authoritative trust servers may be responsible for trust scores for a subset of entities. Merely by way of example, it may be advantageous to divide a plurality of entities based on geographic location of the entity, top level domain ("TLD") of the entity, etc., and to provide an authoritative trust server responsible for each of these divisions. Alternatively and/or in addition, some embodiments may provide multiple authoritative trust servers, each of which is adapted to a particular locale and/or language.

[0093] Hence, there are a variety of ways in which multiple authoritative trust servers may be implemented. In accordance with embodiments of the invention, then, a root server and/or a local trust cache may be configured to include pointers to the appropriate authoritative trust server(s), depending on the score desired (e.g., on the type of behavior, the language, the location of the client and/or the entity being looked up, on the scale desired, etc.).

[0094] In some embodiments, to facilitate rapid transfer of trust scores upon request, trust scores for online entities may be associated with a particular type of identifier of the online entities, such as a domain name or IP address. Other structures may also be used to distribute trust scores. In some cases, trust evaluation system 540 may have sole authority to create and modify trust score(s) to enhance the security of scoring information. Additionally, cache entries maintained in server caches 532 and/or local caches 512 may expire after a predetermined time in order to reduce the use of outdated scores in making decisions about communications from online entities.

[0095] According to one set of embodiments, each trust score server 530 at a hierarchical level below the trust evaluation system 540 may be responsible for a particular set of online entities. In some embodiments, sets of online entities may be determined based on predictive caching algorithms. Other methods may also be used to segregate online entities. When initially populating and/or updating server caches 532 maintained by trust score servers 530, trust evaluation system 540 may only distribute trust scores(s) to a trust score server 530 that are associated with the online entities for which the respective trust score server 530 is responsible. Trust score servers 530 at a higher hierarchical level 530 may distribute its entries or a subset of its entries to additional trust score servers at a lower hierarchical level. If a trust score server 530 receives a request for an entry that is not included in its cache 532, the request may be passed up to the next hierarchical score server 530. The authoritative server may be trust evaluation system 540. When entries are passed back down, they may be cached 532 by the trust score server(s) 530 through with the entries are passed.

[0096] Figure 6 illustrates a second exemplary embodiment of a system that may be used to distribute trust data. Trust evaluation system 620 may evaluate and create trust scores for online entities as previously described. A trust data store (not shown) may maintain trust scores that are associated with an IP address and/or a domain name. In some embodiments, an IP address and/or domain name may be associated with a plurality of trust scores, such as an overall score and any of the additional types of trust scores described above. The trust scores associated with IP addresses and/or domain names may be transmitted by trust evaluation system 620 to a DNS system 610.

[0097] One or more servers in DNS system 610 may maintain DNS records that include the trust scores and/or point to an authoritative source for such scores. These may be,

for example, standard DNS records that have been modified to include a trust score. Of course, based on the disclosure herein, one skilled in the art will appreciate that access controls may be implemented to allow an entity to update that entity's standard DNS information but not to allow unauthorized updates or modifications of the trust scores. Upon receiving a DNS lookup request, a DNS server may transmit one or more trust scores associated with the IP address to a requesting client application 602. Client application 602 may then use the trust score(s) to determine whether to allow, block, quarantine, warn, or take other action on communications associated with the online entity 630.

[0098] Figure 7 illustrates an exemplary system that may be used to implement trust policies. Once a trust score for an online entity has been retrieved by monitoring agent 702 and/or other component, a policy agent 710 may be used to determine one or more actions to apply to communications associated with the online entity. By way of example, actions a policy agent may take include blocking a communication, allowing a communication, quarantining a communication, and/or warning a user of client application 730, an administrator, or other person or computer application. Policy agent 710 may apply actions to outbound communications from a client application 730 to an online entity and/or inbound communications received from an online entity.

[0099] Policy agent 710 may be a standalone program and/or a component of a larger program, such as an operating system, email application, a gateway application, or a web browser application, as described in more detail above. Thus, in some embodiments, policy agent 710 may be implemented on a client computer which executes client application. In other embodiments, policy agent 710 may be implemented on a border device, such as an enterprise router, a proxy server, a firewall server, or any other computer. A policy agent 710 may provide a variety of policies (and/or there may be a plurality of policy agents 710) designed to take different actions based on specific categories of scores and/or to provide application-specific behavior based on a given score. Merely by way of example, a given score may be treated differently in different circumstances--a pornography score of 3 may be assigned a more restrictive policy than a spam category of 3, for example, and/or an email message from an entity accorded a spam score of 4 might be quarantined or blocked, while a web page from the same entity might be allowed.

[0100] One of the actions taken by policy agent 710 may be to quarantine communications. Hence, the system may include a quarantine area 740. Quarantine area 740

may provide a safe area for users, administrators, and/or others to view communications. Alternatively, access to the quarantine area 740 may be restricted to administrative or authorized users. Quarantine area 740 may provide a "sandbox", as is known in the art, to allow the safe execution of email attachments, scripts, web pages and/or the like. Hence, the quarantine area 740 can allow "locked down" access to quarantined data, allowing a user (and/or another) to access the data without exposing the system to potential threats contained within the data.

[0101] In some aspects, policy agent 710 may determine the action(s) to take based on one or more policies 712. Policies 712 may define actions to be taken based on ranges or threshold score values. By way of example, in embodiments using the 1-5 scoring system previously described, policies 712 may indicate that communications to and/or from online entities with a trust score of 5 (disreputable) are blocked or dropped. A trust score of 4 may be associated with a policy 712 to quarantine communications from the online entity, while a trust score of 3 may be associated with a policy 712 to warn a user, administrator, or other party or system. Policies 712 may further indicate that communications associated with online entities having a trust score of 1 or 2 are allowed (passed). It should be appreciated that in other embodiments, policies 712 may include different types of policies, which may vary based on the scoring system used to evaluate the trustworthiness of online entities. Additionally, some embodiments may include policies 712 which make use of additional trust scores (e.g., a fraud trust score, an unwanted traffic trust score), e.g., to take specific actions based on the threat implied by the additional trust score(s). Moreover, as mentioned above, while the exemplary 1-5 scoring scheme is designed to be efficient, it may be expanded, contracted and/or otherwise modified in specific implementations.

[0102] Figure 8 illustrates an exemplary method that may be used to evaluate a communication and/or to obtain trust data. Communication traffic to and/or from one or more client applications may be monitored 802 at the client, a border device, or other system. If an inbound and/or outbound communication associated with an online entity is detected 804, at least one trust score associated with the online entity is obtained as described in blocks 808-812. Otherwise, monitoring 802 of communication traffic may continue. In other embodiments, communication traffic may not be monitored 802. Instead, the client application may detect 804 the inbound or outbound communication and may then obtain or request the trust score.

[0103] In one set of embodiments, the trust score may be obtained by first determining 806 if a local trust cache includes the trust score. If the trust score is cached (and is not expired), the trust score is retrieved 808 from the local trust cache. Otherwise, a request for the trust score may be requested 810 from a trust score server.

[0104] The trust score server to which the request is sent may be responsible for providing trust scores to the computer (e.g., client computer, gateway computer) associated with the requester. As previously described, if a cache associated with the trust score server does not include the requested trust score, the trust score server may issue a request to another trust score server and/or trust evaluation system to obtain the requested trust score. Any of the trust score servers and/or the trust evaluation system itself may transmit the trust score back to the requesting computer. In one set of embodiments, the trust score and/or a pointer to the appropriate trust score server may be transmitted back down the hierarchical chain, which may provide for the caching of the trust score for future requests. In an aspect, a trust score request might use the following priority: First a request is made to a peer server; if no trust information is found, a request may be made to a higher-level server. This process can continue until a request is made to a known authoritative server (or root server, if appropriate). In some cases, a server at each level of the hierarchy might proxy for servers (and/or clients) at lower levels of the hierarchy in making requests to higher levels of the hierarchy. In such cases, the ultimate response to the request can then be propogated back down the hierarchy, and caches at each level may be updated if appropriate.

[0105] Once the trust score has been retrieved 810 or received 812 at the computer requesting the trust score, the score may be transmitted 814 to a policy agent (which may be a separate program or a component of a program which obtained the trust score). Policy agent may then determine action(s) to apply to the communication associated with the online entity.

[0106] It should be appreciated that in alternative embodiments, trust scores may be acquired using a process different than that described with reference to Figure 8. For example, the trust score may be acquired from a DNS record. Other processes may also be used.

[0107] Figure 9 illustrates an exemplary method that may be used to implement trust policies. A trust score associated with an online entity may be received 902 by a policy agent. A policy agent may be a component of an operating system, a web browser

application, an email application, a gateway application, and/or any other type of application (including those discussed above), and/or may be a standalone application. In one set of embodiments, one or more trust policies may be retrieved 904 and applied based on the trust score.

[0108] Trust policies retrieved 904 may indicate action(s) to apply to a communication associated with the online entity based on the trust score. In some aspects, trust policies may be applied by comparing the trust score to one or more values associated with a trust policy. Merely by way of example, if an allow policy condition is satisfied 906, the communication may be allowed. Before passing the communication, the method may also include evaluating a warning policy to determine whether a warning should be attached to the communication. If a condition associated with a warning policy is satisfied 908, a warning to a user may be transmitted 916. With or without the warning, the communication may then be passed 914 either to the online entity (if it was an outbound request) or to a client application (if it was an inbound communication received from the online entity). Some embodiments may provide an option to the user receiving the warning to block and/or quarantine the communication before it is passed 914.

[0109] If the allow condition was not satisfied 906, additional policies may be evaluated to determine the action to apply to a communication. Merely by way of example, if a condition associated with a quarantine policy is satisfied 910, the communication may be quarantined 918. Optionally, the client application and/or user associated with the communication (either initiating or receiving the communication from the online entity) may be notified the communication was quarantined. If the allow policy conditions are not satisfied and the quarantine policy conditions are not satisfied, the communication may be blocked 912 and/or dropped (filtering for interests and/or preferences can work in a similar way). The client application, user, sender, and/or other party may be notified that the communication was blocked 912.

[0110] In alternative embodiments, trust policies may be implemented differently than described with reference to Figure 9. For instances, additional, fewer, or different policies may be applied to a trust score and/or policies may be applied in a different order. Other variations are also contemplated.

[0111] It should be appreciated that trust scores which evaluate the trustworthiness and/or reputation of online entities have a wide range of applications. For exemplary purposes, consider a situation in which a server attempts to send an email message to a user using a mail client on a user computer. The sending server routes the message (usually via the Internet) to the mail server for the user's ISP (or corporation, etc.). In accordance with embodiments of the invention, the mail server, upon receiving the message, examines the message to determine an identifier (such as a host, domain, IP address, etc.) of the sending server. The mail server then queries a local trust caching database for scoring (or other) information about the sending server. If the caching database has relevant information that has not expired, the caching database (and/or a server associated therewith), transmits this information to the mail server. If the caching database does not have the requested information (or has an expired version of the information), the caching database (or, again, a server associated therewith), may refer the mail server to, and/or forward the request to, an authoritative database, a root database or server, etc., perhaps in a fashion similar to the caching and retrieval methods implemented by DNS systems (perhaps with some modification, such as the provision of an entire score database to one or more core servers), and such a database or server provides the requested information, either to the caching database and/or the mail server. Upon receiving the scoring information, the mail server (e.g., a policy agent component of the mail server) may make a determination of how to handle the message, including without limitation any of the options mentioned above. In some aspects, if scoring information is not available, the mail server may assume the sender is disreputable (or reputable).

[0112] As a second example, when a user (using a client application, such as a web browser) attempts to access a web page at a web server, a proxy server (e.g., a monitoring agent component of the proxy server), before transmitting the HTTP request (and/or the response from the server), may consult a caching database in a manner similar to that mentioned above. Based on trust scoring information received, the proxy server may determine an appropriate action to take, including without limitation any of the actions mentioned above.

[0113] Alternative configurations are possible as well. Merely by way of example, it may be more appropriate in some situations (such as when a client and mail server are configured with a POP3 relationship, and/or when a client does not use a proxy server to

access the Internet), for software on the client to obtain trust scores and determine actions to apply to communications based on the trust scores. For instance, a software firewall on a client could be configured to limit incoming and outgoing transmissions according to a trust score accorded the transmitting/receiving server, domain, etc. Alternatively and/or in addition, other types of applications (such as mail clients, web browsers, etc.) may also be configured (e.g., through options, plug-ins, tool bars, etc.) to use trust scores.

[0114] Other applications of the present invention are possible as well, including integration with additional systems. For instance, the Anti-Fraud Applications disclose a number of fraud prevention and/or detection systems, which embodiments of the present invention may incorporate, and/or embodiments of the invention may be integrated with, and/or be operated in conjunction with such systems. Merely by way of example, an exemplary system disclosed by the Anti-Fraud Applications is a system designed to monitor records modified in or added to a zone file and monitor any domains associated with the added/modified records for activity. A set of embodiments of the present invention may be integrated with such systems. For example, if a new domain record is found in the monitoring of a zone file, the trust score of one or more entities associated with the new domain record (e.g., an owner of the new domain, an enabling party for the new domain, etc.) may be provided by an embodiment of the present invention. Depending on the trust score, then, a determination may be made regarding whether the new domain presents a likely threat of illegitimate activity (such as phishing, trademark misuse, cybersquatting, etc.), and the trust score of the associated entities may be used to inform a decision whether (and/or how) to monitor the new domain for activity.

[0115] Merely by way of example, if a new domain is registered by an entity with a high trust score (indicating a relatively low probability of illegitimate activity), the domain may be monitored relatively less aggressively and/or may not be monitored at all. In contrast, if an entity with a relatively low trust score (and/or an unknown entity) registers a domain, that entity's trust score (and/or lack thereof) may prompt a decision to monitor the trust score relatively more aggressively, especially if the domain is associated with one or more enabling parties (such as registrars, ISPs, etc) having relatively low trust scores.

[0116] Conversely, various systems integrated with embodiments of the invention (and/or operated in conjunction with embodiments of the present invention) may be used to provide data sources for a trust database, as discussed above. Merely by way of example, if

the monitoring system of the previous example determines that a new domain is involved in illegitimate activity (such as phishing, cybersquatting, etc.), that determination may be used as data to calculate and/or update one or more trust scores for the entity operating the domain and/or any associated entities (which could include enabling parties, affiliated entities, and the like).

[0117] An identity tracking system, such as the systems disclosed in the Online Identity Tracking Application, may be integrated, incorporated and/or operated in conjunction as well. For instance, in the examples above, an identity tracking system may be used to identify an entity registering and/or operating a new domain, and/or any associated entities (which, again, could include enabling parties, affiliated entities, etc.), and/or to provide data for the development and/or update of a trust score for the entity.

[0118] Merely by way of example, if a new domain is registered (and/or ownership or other information for a domain is modified), the registration record may be parsed for pertinent information (which can be any information that may be used to identify an entity associated with the domain registration, such as corporate name, contact name, address, telephone number, contact email address, etc.), and such information may be used as input to an identity tracking system. The identity tracking system, then, may search for such information and/or related information in an identity tracking database (as disclosed in the Online Identity Tracking Application, for example). Such information thus may be used to identify records related to one or more entities associated with the new domain (including without limitation the owner of the domain, any associated and/or affiliated parties, enabling parties, etc.).

[0119] The identity tracking system may also be used for additional diagnostic purposes. In a particular case, for example, if the new domain name registration is for a domain name similar to the name of a client of the trust provider (which may indicate that the new domain might be used for cybersquatting, phishing and/or some other unsavory activity), the identity tracking system can search the identified records for any records indicating ownership of (and/or any other association with) any other similar domains (such as domain names related and/or similar to the customer's brand name(s), domain name(s) and/or trademark(s); the customer's industry; other companies in the customer's industry; etc.), which may indicate that an entity associated with the new domain registration is engaging in

a practice of acquiring such domains, a possible indicator that the entity is engaging in (and/or plans to engage in) one or more illegitimate activities.

[0120] This indication may be used in several ways. First, a notification may be provided to an operator of the identity tracking system, the trust evaluation system and/or another that further investigation and/or monitoring may be appropriate. Alternatively and/or in addition, such monitoring and/or investigation may be undertaken automatically (using, for example, one or more of the systems described in the Anti-Fraud Applications). In particular embodiments, an event may be created in an event manager (described in detail in the Anti-Fraud Applications), allowing for the initiation, tracking and/or management of any appropriate fraud detection and/or prevention processes.

[0121] Second, one or more trust scores of any associated entities may be updated, using, for example, methods described above. Alternatively and/or in addition, one or more records may be updated in the identity tracking system to indicate an association and/or correlation between the owner of the new domain (as well as any affiliated parties, enabling parties, etc.) and entities identified by the identity tracking system as associates of those entities.

[0122] There are additional applications of embodiments of the present invention as well. Merely by way of example, implementations might include the use of a toolbar, plug-in, and/or the like that could be integrated and/or used with a client application (including without limitation those client applications discussed above, such as web browsers, electronic mail clients, instant messaging and/or internet chat clients, and the like). As mentioned above, a toolbar might be configured (using a policy manager and/or other software component) to obtain trust scores for entities with whom a user communicates using the client application. Alternatively and/or in addition, a toolbar (and/or any other software component, such as a firewall application, client application, etc.) might be configured to implement whitelists, blacklists and/or greylists, which might be based on trust scores for various listed entities. In a particular set of embodiments, a toolbar (and/or another component) might be configured to receive a list of entities compiled by a trust server, root server and/or any other of the systems described above, based on the trust scores of those entities. Entities scored with a 1, for example, might be added to a whitelist, while entities scored with a 4 or 5 might be added to a blacklist. Such toolbars and components can also be

used to provide filtering by preference and/or interest, based on interest scores assigned to various entities and/or communications.

[0123] In one aspect, one or more greylist(s) might be implemented as well, which could include entities scored with a 3 and/or entities associated (perhaps to a degree specified by a user, administrator and/or a trust provider) with entities scored with a 4 or a 5. Merely by way of example, if an entity is scored with a 5 (meaning the entity is relatively untrustworthy), any closely-associated entities (which might be defined to mean any entities with the same telephone number, contact email address, etc.) are added to a greylist. (Of course, based on the disclosure herein, one skilled in the art will appreciate that a variety of criteria may be used to defined the degree of association that will cause an entity to be placed on a greylist.) In another set of embodiments, the scoring system might be unnecessary. Merely by way of example, if an entity is known (e.g., by a trust provider) to have engaged in fraud, that entity might be added to a blacklist, and/or any entities associated (to whatever degree is deemed appropriate) with that entity might be added to a greylist.

[0124] In a particular set of embodiments, a plurality of greylists may be supported. Merely by way of example, a first greylist might comprise entities known to be associated with blacklisted entities, as discussed above. A second greylist might comprise entities suspected (but perhaps not known) to engage in illegitimate activities and/or unwanted communications. Further, there may be a plurality of blacklists, whitelists and/or greylists corresponding to various behavior characteristics and/or categories of activities, including without limitation those categories and/or characteristics discussed above. Merely by way of example, there may be a first list (and/or set of lists--black, white and/or grey) related to entities' likelihood to transmit spam, a second list (and/or set of lists) related to entities' likelihood to be purveyors of pornography, a third list (and/or set of lists) related to entities' likelihood to be engaged in legitimate online commerce, etc. These lists may be used by a user, administrator, etc. to customize the behavior of one or more client applications with respect to entities on the various lists.

[0125] The toolbar (or other component) then, might be configured to automatically allow access to communications (e.g., email messages, web pages, etc.) with whitelisted entities, automatically block access to communications with blacklisted entities, and/or to take some other action with respect to communications with greylisted entities. Other actions, including those discussed above, such as warning, quarantining, etc. are possible as

well. If desired, a policy manager (and/or filtering engine) might be used to define the behavior of a toolbar (or other component) with respect to each type of entity. In some cases, a user might be given the ability to modify the blacklist, whitelist and/or greylist (e.g., by adding or removing entries manually, and/or by selecting an option--from a toolbar button, context menu, and/or the like--when viewing a communication from a given entity, to add that entity to a blacklist, whitelist or greylist) and/or to modify the application's behavior with respect to each type of list. In other cases, the lists (and/or the application's behavior) might be administratively controlled by a local administrator, a trust provider, etc.

[0126] In accordance with particular embodiments, the toolbar (or other component) might be fed updates automatically from a central location (e.g., a trust evaluation system) and/or through a distributed network of caching servers, etc. Updates might be automated at the client and/or the server(s), and/or might be performed on demand as requested by the client. A variety of updating schemes (such as for operating system updates, virus definition updates, etc.) are known in the art, and any of these updating schemes may be used as appropriate in accordance with various embodiments.

[0127] In the foregoing description, for the purposes of illustration, methods were described in a particular order. It should be appreciated that in alternate embodiments, the methods may be performed in a different order than that described. Additionally, the methods may include fewer, additional, or different blocks than those described. It should also be appreciated that the methods described above may be performed by hardware components or may be embodied in sequences of machine-executable instructions, which may be used to cause a machine, such as a general-purpose or special-purpose processor or logic circuits programmed with the instructions to perform the methods. These machine-executable instructions may be stored on one or more machine readable mediums, such as CD-ROMs or other type of optical disks, floppy diskettes, ROMs, RAMs, EPROMs, EEPROMs, magnetic or optical cards, flash memory, or other types of machine-readable mediums suitable for storing electronic instructions. Alternatively, the methods may be performed by a combination of hardware and software.

[0128] In conclusion, the present invention provides novel solutions for evaluating the trustworthiness of various online entities, and for distributing and/or using such information. While detailed descriptions of one or more embodiments of the invention have been given above, various alternatives, modifications, and equivalents will be apparent to

those skilled in the art without varying from the spirit of the invention. Moreover, except where clearly inappropriate or otherwise expressly noted, it should be assumed that the features, devices and/or components of different embodiments can be substituted and/or combined. Thus, the above description should not be taken as limiting the scope of the invention, which is defined by the appended claims.

WHAT IS CLAIMED IS:

1. A method comprising:

receiving, at a computer, a trust score score evaluating a trustworthiness of an online entity;

consulting, with the computer, at least one trust policy; and

determining an action to take based at least in part on the trust policy and the trust score; and

taking the action with respect to a communication associated with the online entity.

2. The method of claim 1, wherein determining the action to take comprises comparing the trust score to one or more values associated with the trust policy.

3. The method of claim 1, wherein the trust score is one of a plurality of trust scores for the online entity.

4. The method of claim 3, wherein the plurality of trust scores comprises one or more scores selected from a group consisting of: a trust score evaluating the likelihood of the online entity to engage in fraudulent behavior, a trust score evaluating the likelihood of the online entity to transmit unwanted communications, a trust score evaluating the likelihood of the online entity to engage in cybersquatting, and a trust score evaluating the likelihood of the online entity to engage in trademark abuse.

5. The method of claim 3, wherein the trust score is a first trust score of the plurality of trust scores, the first trust score evaluating the trustworthiness of the online entity in a first category of behavior, the method further comprising:

receiving, at the computer, a second trust score of the plurality of trust scores evaluating the trustworthiness of the online entity in a second category of behavior.

6. The method of claim 1, wherein the action comprises blocking the communication.

7. The method of claim 6, wherein blocking the communication comprises blocking a communication received from the online entity.

8. The method of claim 6, wherein blocking the communication comprises blocking a communication addressed to the online entity.

9. The method of claim 1, wherein the action comprises quarantining the communication.

10. The method of claim 9, further comprising transmitting a notification indicating the communication was quarantined.

11. The method of claim 1, wherein the action comprises allowing the communication.

12. The method of claim 1, wherein the action comprises transmitting a warning to a recipient of the communication.

13. The method of claim 1, wherein the communication comprises a communication received from the online entity.

14. The method of claim 1, wherein the online entity is an intended recipient of the communication.

15. The method of claim 1, wherein the computer is a client computer.

16. The method of claim 1, wherein the computer is a border device.

17. A trust authentication system comprising:

a data store including one or more trust policies; and

a first software component on a computer, configured to monitor communications associated with one or more client applications for a communication with an online entity;

a second software component on the computer, configured to obtain one or more trust scores associated with an online entity; and

a third software component on the computer, configured to take an action with respect to the communication with the online entity, based on at least one of the one or more trust scores associated with the online entity and at least one of the one or more trust policies.

18. The trust authentication system of claim 17, wherein the first, second and third software components execute on a border device separate from a client computer executing the one or more client applications.

19. The trust authentication system of claim 17, wherein the first, second and third software components execute on a client computer executing the one or more client applications.

20. The trust authentication system of claim 17, wherein the first and second software components are incorporated within a monitoring agent.

21. The trust authentication system of claim 17, wherein the third software component comprises a policy agent.

22. The trust authentication system of claim 17, wherein at least one of the software components is integrated within at least one of the one or more client applications.

23. The trust authentication system of claim 17, wherein at least one of the software components is integrated within an operating system of the computer.

24. The trust authentication system of claim 17, wherein the first, second and third software components are integrated within an application program separate from the one or more client applications.

25. The trust authentication system of claim 17, wherein at least one of the software components is incorporated within a software program configured to operate in conjunction with at least one of the one or more client applications.

26. The trust authentication system of claim 25, wherein the software program is selected from the group consisting of: a toolbar, a plug-in, and an extension.

27. The trust authentication system of claim 17, further comprising a quarantine area to store quarantined communications, wherein the action comprises quarantining the communication in the quarantine area.

28. A trust authentication system comprising a processor and instructions executable by the processor to:

monitor communications associated with one or more client applications for a communication with an online entity;

obtain one or more trust scores associated with an online entity; and

take an action with respect to the communication with the online entity, based on at least one of the one or more trust scores associated with the online entity.

29. A trust authentication system comprising a processor and instructions executable by the processor to:

monitor a plurality of communications associated with a plurality of client computers;

identify an online entity other than one of the client computers, the online entity being associated with one of the plurality of communications;

obtain one or more trust scores associated with the online entity; and

take an action with respect to the one of the plurality of communications, based on at least one of the one or more trust scores associated with the online entity.

30. The trust authentication system of claim 29, wherein the processor is incorporated within a border device.

31. A software program embodied on a computer readable medium, the software program comprising instructions executable by a computer to:

receive a trust score evaluating a trust of an online entiy;

based on the trust score, take an action with respect to a communication associated with the online entity.

32. A software program embodied on a computer readable medium, the software program comprising instructions executable by a computer to:

monitor communications associated with one or more client applications for a communication with an online entity;

obtain one or more trust scores associated with an online entity;

consult at least one trust policy; and

take an action with respect to the communication with the online entity, based on at least one of the one or more trust scores associated with the online entity.

33. A software program embodied on a computer readable medium, the software program comprising instructions executable by a computer to:

monitor a plurality of communications associated with a plurality of client computers;

identify an online entity other than one of the client computers, the online entity being associated with one of the plurality of communications;

obtain one or more trust scores associated with the online entity; and

take an action with respect to the one of the plurality of communications, based on at least one of the one or more trust scores associated with the online entity.

34. A system comprising:

means for monitoring communications associated with one or more client applications for a communication with an online entity;

means for obtaining one or more trust scores associated with an online entity;

means for consulting at least one trust policy; and

means for taking an action with respect to the communication with the online entity, based on at least one of the one or more trust scores associated with the online entity and the at least one trust policy.

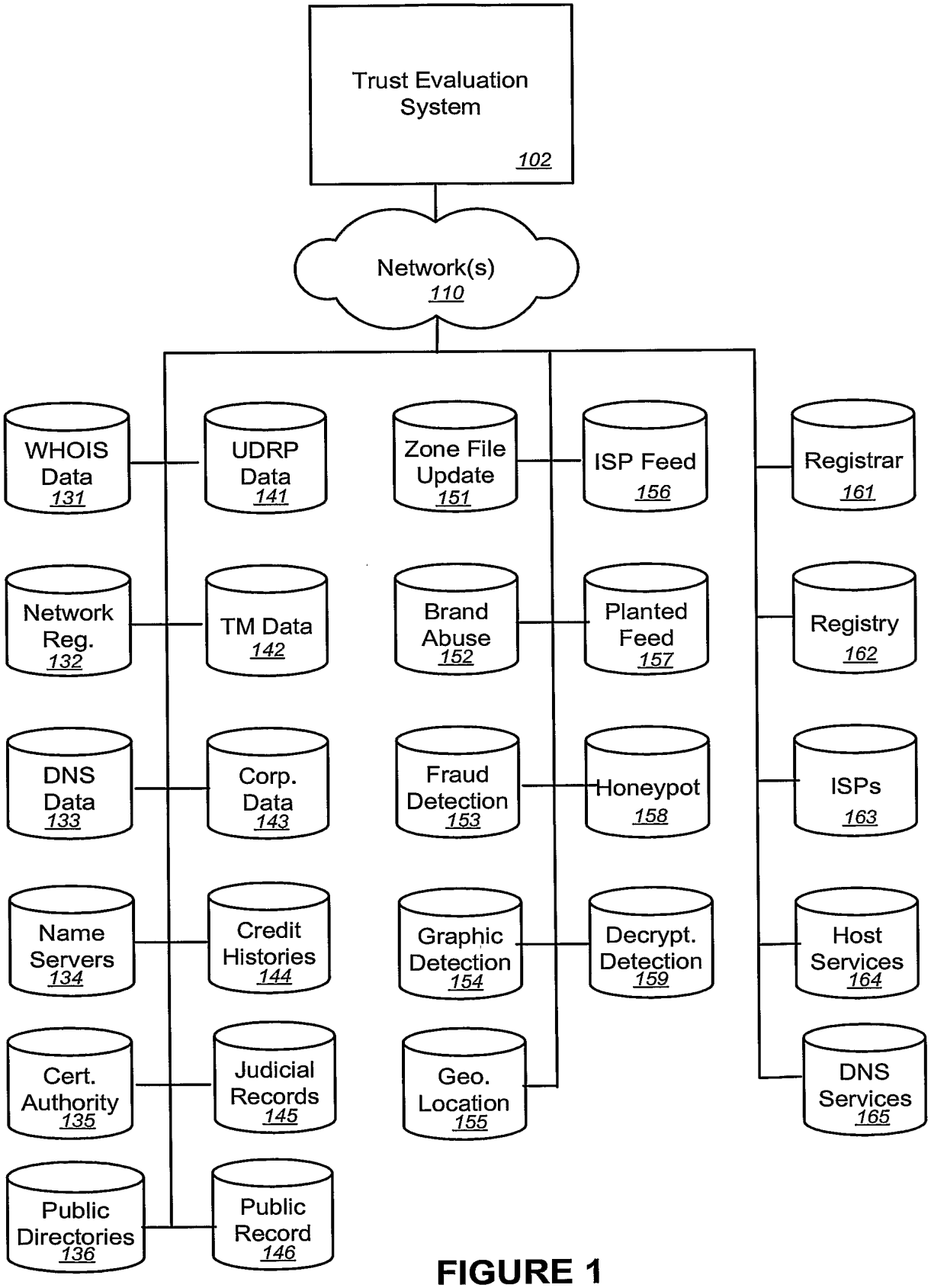

Trust Evaluation System
102
Network(s)
110
WHOIS Data
131
UDRP Data
141
Zone File Update
151
ISP Feed
156
Registrar
161
Network Reg.
132
TM Data
142
Brand Abuse
152
Planted Feed
157
Registry
162
DNS Data
133
Corp. Data
143
Fraud Detection
153
Honeypot
158
ISPs
163
Name Servers
134
Credit Histories
144
Graphic Detection
154
Decrypt. Detection
159
Host Services
164
Cert. Authority
135
Judicial Records
145
Geo. Location
155
DNS Services
165
Public Directories
136
Public Record
146

FIGURE 1

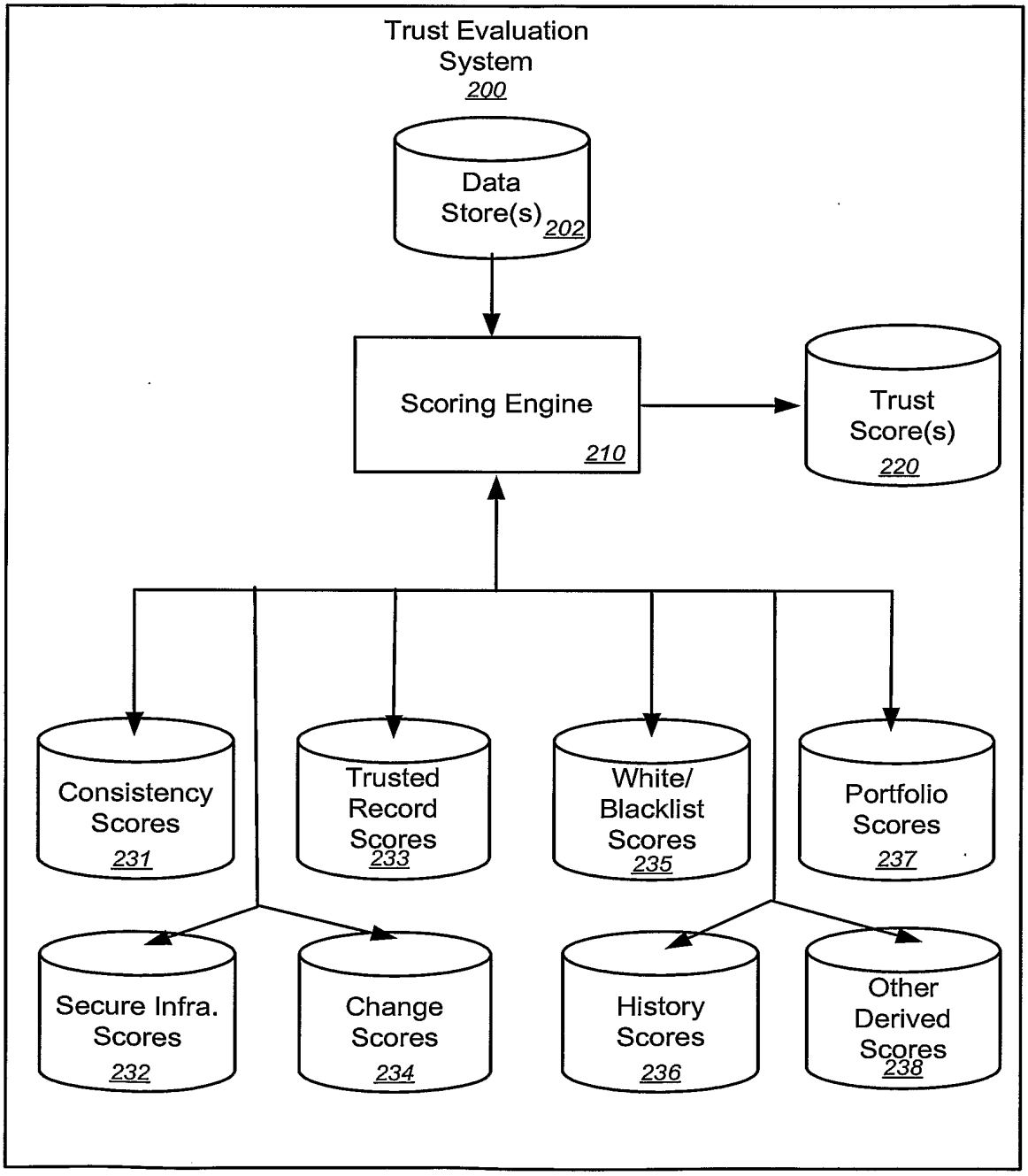

Trust Evaluation System
200
Data Store(s)
202
Scoring Engine
210
Trust Score(s)
220
Consistency Scores
231
Trusted Record Scores
233
White/ Blacklist Scores
235
Portfolio Scores
237
Secure Infra. Scores
232
Change Scores
234
History Scores
236
Other Derived Scores
238

FIGURE 2

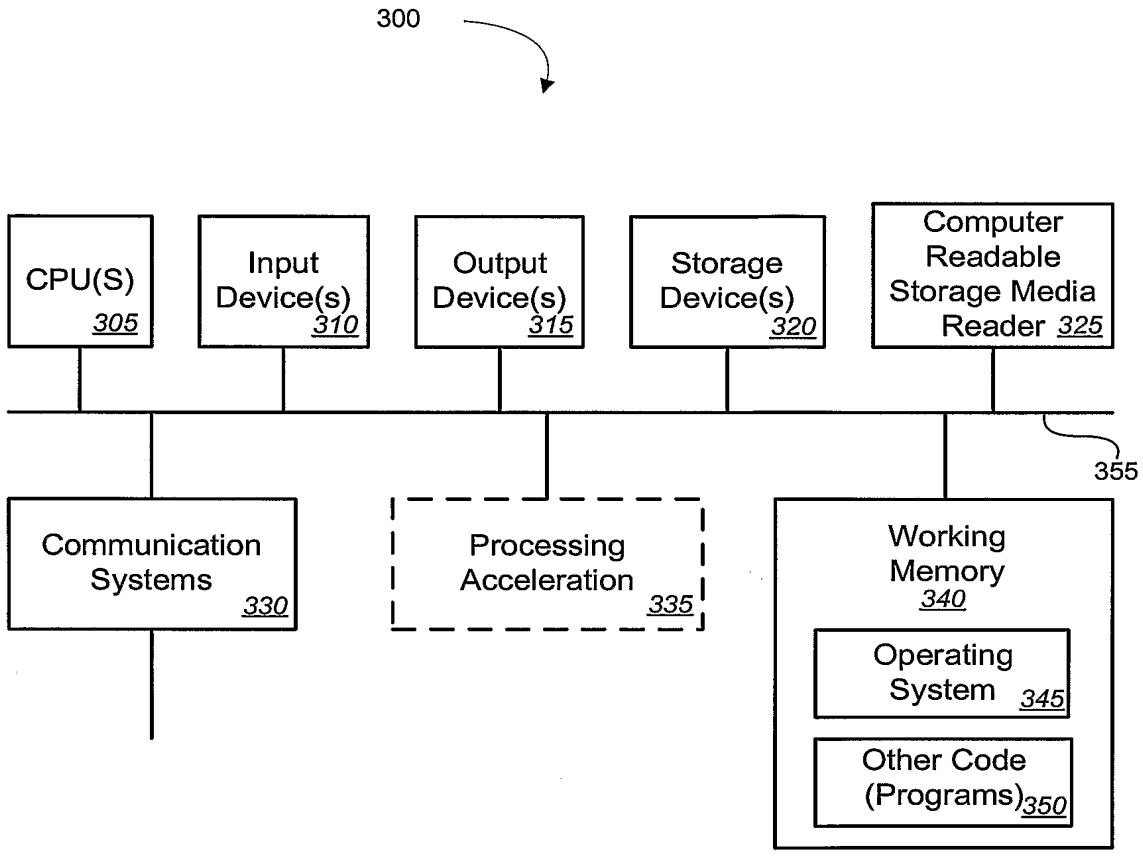

300
CPU(S) 305
Input Device(s) 310
Output Device(s) 315
Storage Device(s) 320
Computer Readable Storage Media Reader 325
355
Communication Systems 330
Processing Acceleration 335
Working Memory 340
Operating System 345
Other Code (Programs) 350

FIGURE 3

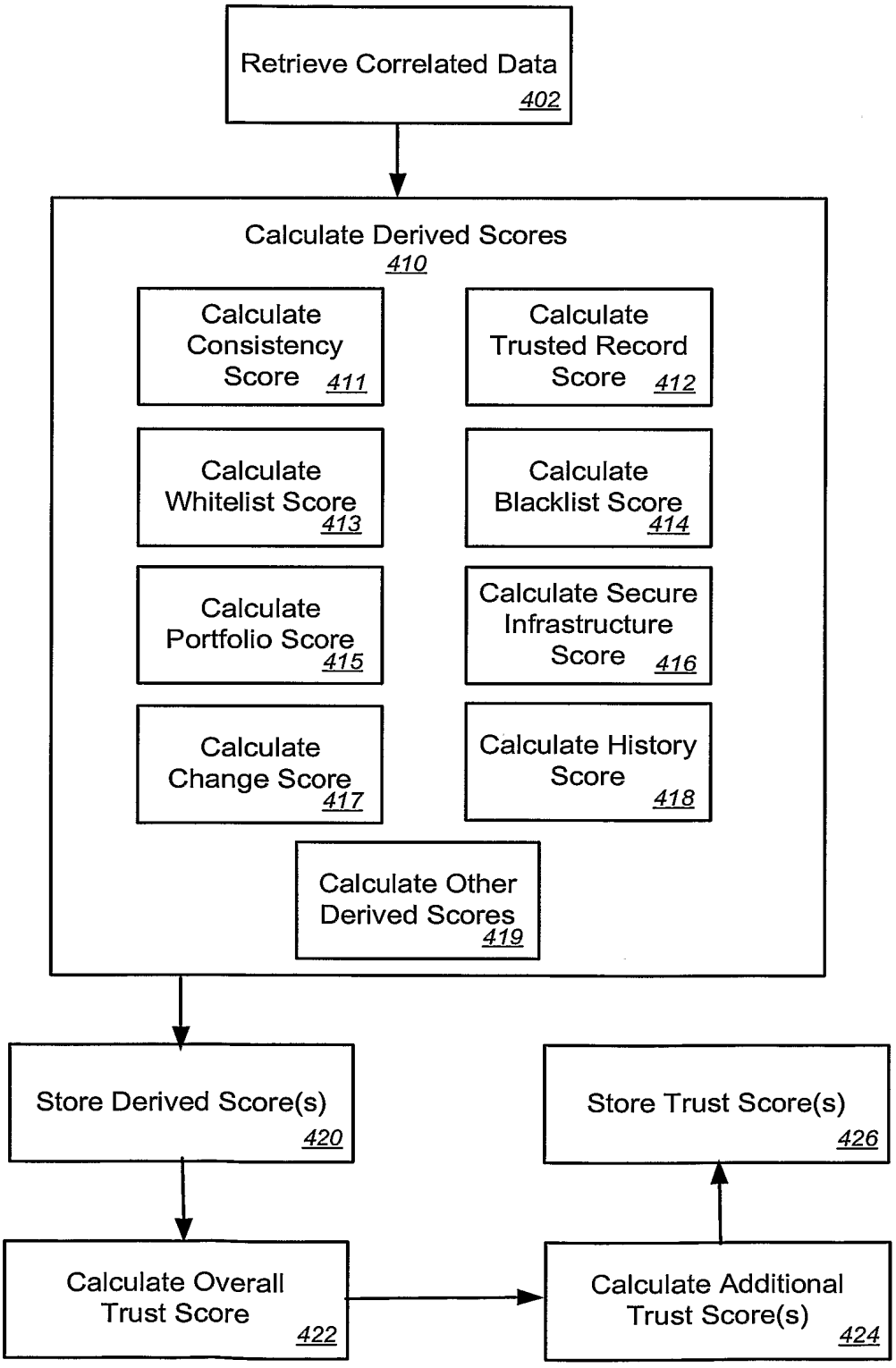

Retrieve Correlated Data
402
Calculate Derived Scores
410
Calculate Consistency Score 411
Calculate Trusted Record Score 412
Calculate Whitelist Score 413
Calculate Blacklist Score 414
Calculate Portfolio Score 415
Calculate Secure Infrastructure Score 416
Calculate Change Score 417
Calculate History Score 418
Calculate Other Derived Scores 419
Store Derived Score(s) 420
Store Trust Score(s) 426
Calculate Overall Trust Score 422
Calculate Additional Trust Score(s) 424

FIGURE 4

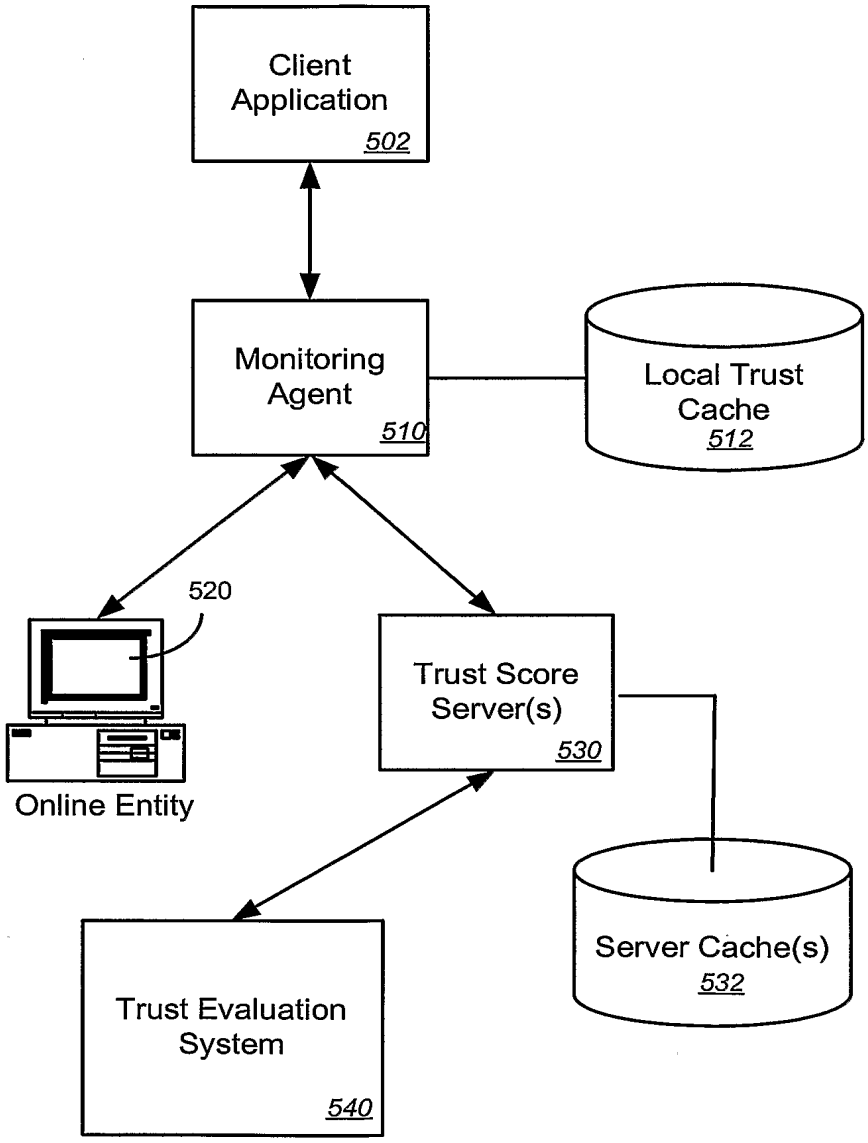

Client Application
502
Monitoring Agent
510
Local Trust Cache
512
520
Online Entity
Trust Score Server(s)
530
Server Cache(s)
532
Trust Evaluation System
540

FIGURE 5

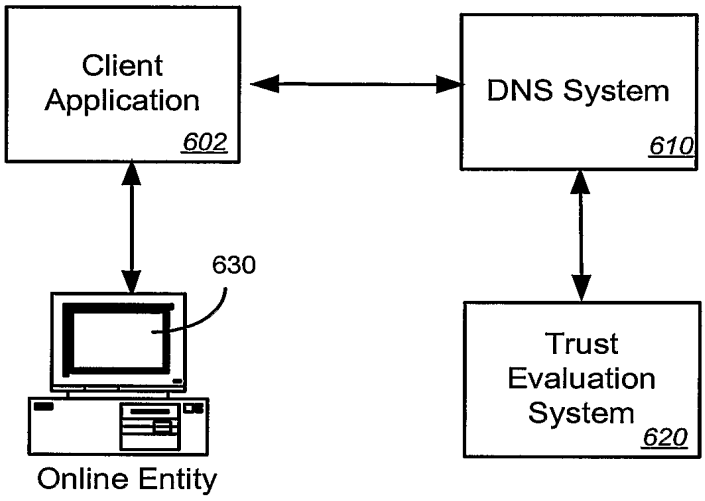


FIGURE 6

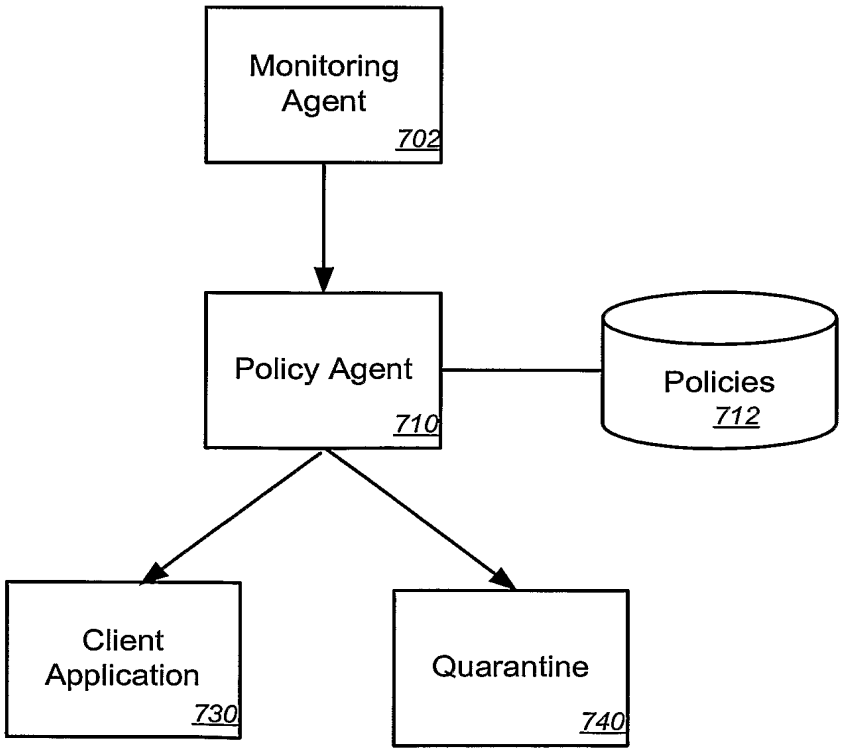


FIGURE 7

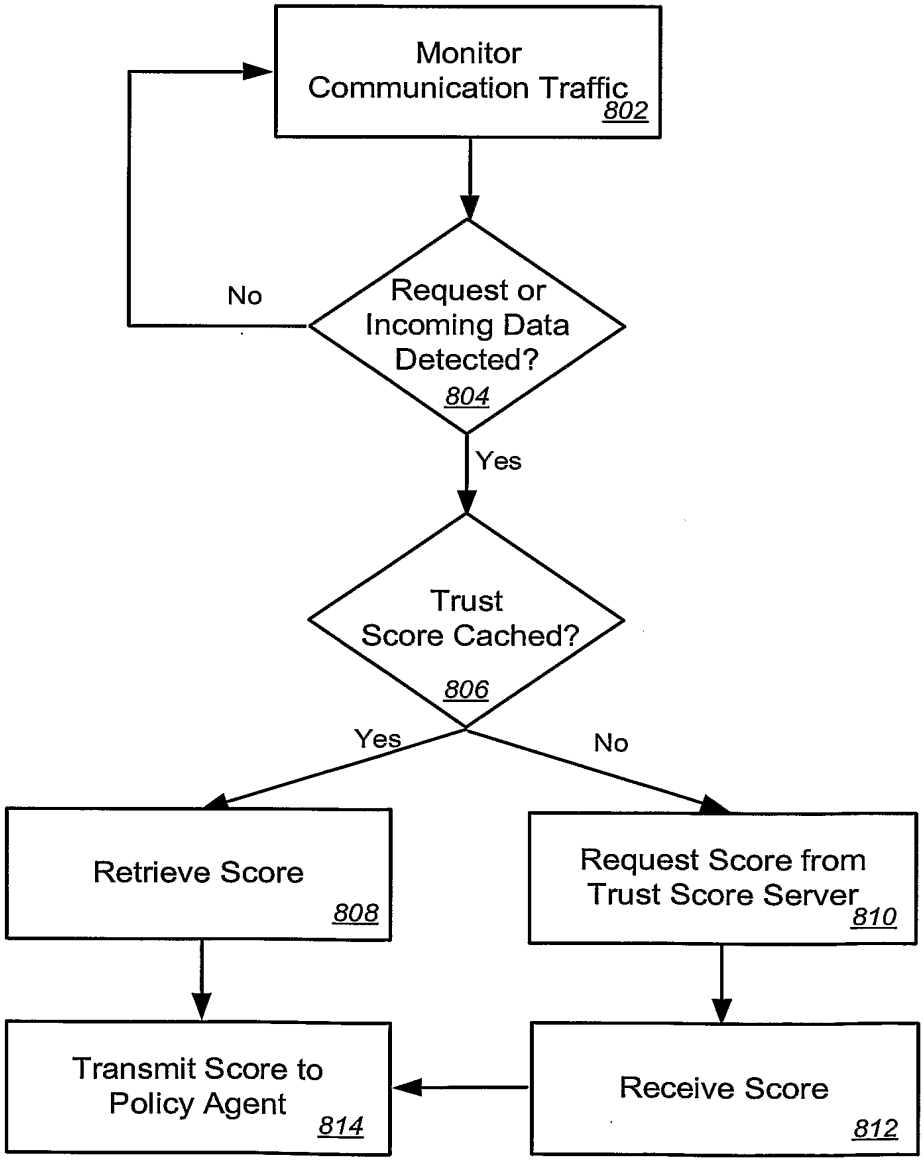

Monitor Communication Traffic
802
Request or Incoming Data Detected?
804
No
Yes
Trust Score Cached?
806
Yes
No
Retrieve Score
808
Request Score from Trust Score Server
810
Transmit Score to Policy Agent
814
Receive Score
812

FIGURE 8

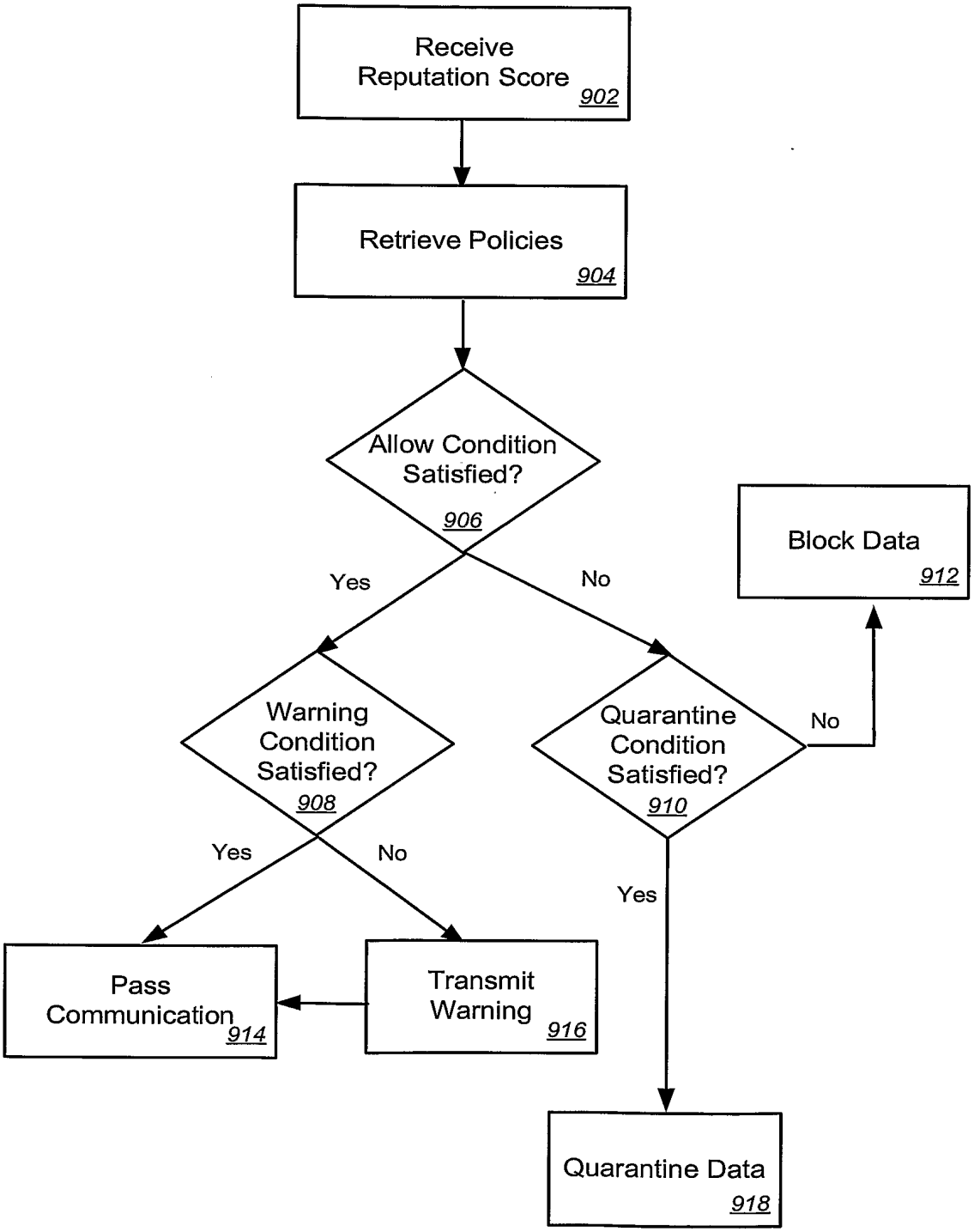

Receive Reputation Score 902
Retrieve Policies 904
Allow Condition Satisfied? 906
Yes
No
Block Data 912
Warning Condition Satisfied? 908
Quarantine Condition Satisfied? 910
No
Yes
No
Yes
Pass Communication 914
Transmit Warning 916
Quarantine Data 918

FIGURE 9

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 August 2012 (23.08.2012)

WIPO | PCT

(10) International Publication Number
WO 2012/110501 A1

(51) **International Patent Classification**:
G06F 21/00 (2006.01)

(21) **International Application Number**:
PCT/EP2012/052497

(22) **International Filing Date**:
14 February 2012 (14.02.2012)

(25) **Filing Language**: English

(26) **Publication Language**: English

(30) **Priority Data**:
61/443,095 15 February 2011 (15.02.2011) US

(71) **Applicant** *(for all designated States except US)*: **PREVX LIMITED** [GB/GB]; 3 New Park Place, Pride Park, Derby Derbyshire DE24 8DZ (GB).

(72) **Inventors; and**

(75) **Inventors/Applicants** *(for US only)*: **MORRIS, Melvyn** [GB/GB]; Redmire Gap, Intakes Lane, Turnditch, Belper Derbyshire DE56 2LU (GB). **JAROCH, Joseph** [US/US]; 1484 Worden Way, Elk Grove Village, IL 60007 (US).

(74) **Agent**: **BEBBINGTON, Nicholas**; Fulwood House, 12 Fulwood Place, London London WC1V 6HR (GB).

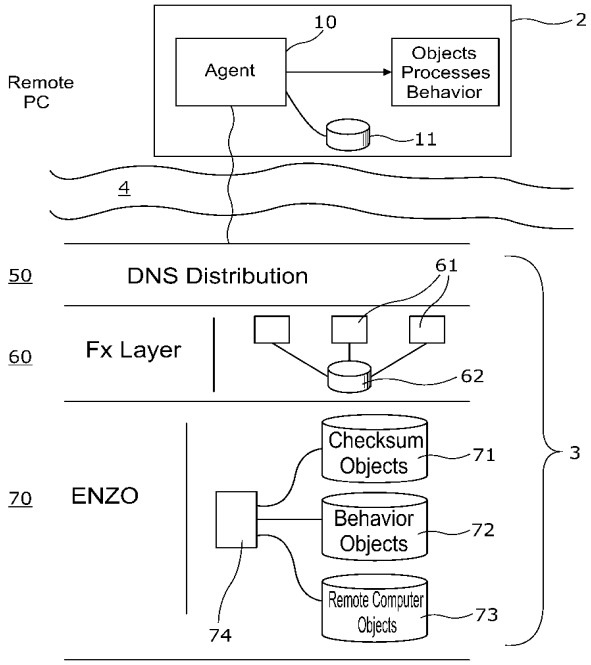
(81) **Designated States** *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) **Designated States** *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) **Title**: METHODS AND APPARATUS FOR DEALING WITH MALWARE

Fig. 3



(57) **Abstract**: In one aspect, a method of classifying a computer object as malware includes at a base computer (3), receiving data about a computer object from each of plural remote computers (2) on which the object or similar objects are stored and or processed. The base computer (3) comprises plural threat servers (62) arranged to receive said data from the plural remote computers (2) and apply rules and or heuristics against that data in real time to determine whether or not said object is malware and to communicate said determination to the remote computers (2). The base computer (3) comprises at least one central server (74) in communication with the threat servers (62) and arranged to receive said data about objects from the threat servers (62) to maintain a master database (71, 72, 73) of data received about objects from all of the threat servers (62).

WO 2012/110501 A1

Published:

— *with international search report (Art. 21(3))*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

METHODS AND APPARATUS FOR DEALING WITH MALWARE

This application claims the benefit of priority to US application serial no. 61/443095, filed February 15th, 2011, the content of which is hereby incorporated by reference.

The present invention relates generally to methods and apparatus for dealing with malware.

In aspects, the present invention relates to a method and computer program for connecting a remote computer to one of a plurality of servers, a method and computer program for providing protection against malware, methods and apparatus for classifying a computer object as malware, a method of operating a security program on a computer, and a computer program for fighting malware.

The term "malware" is used herein to refer generally to any executable computer file or, more generally "object", that is or contains malicious code, and thus includes viruses, Trojans, worms, spyware, adware, etc. and the like.

A typical anti-malware product, such as virus scanning software, scans objects or the results of an algorithm applied to the object or part thereof to look for signatures in the object that are known to be indicative of the presence of malware. Generally, the method of dealing with malware is that when new types of malware are released, for example via the Internet, these are eventually detected. Once new items of malware have been detected, then the service providers in the field generate signatures that attempt to deal with these and these signatures are then released as updates to their anti-malware programs. Heuristic methods have also been employed.

These systems work well for protecting against known malicious objects. However, since they rely on signature files being generated and/or updated, there is inevitably a delay between a new piece of malware coming into existence or being

released and the signatures for identifying that malware being generated or updated and supplied to users. Thus, users are at risk from new malware for a certain period of time which might be up to a week or even more.

More recently, so-called "cloud" based techniques have been developed for fighting malware/viruses. In this technique, protection is provided by signatures that are stored in the cloud, i.e. in a central server to which the remote computers are connected. Thus, a remote computer can be given protection as soon as a new malware object is spotted and its signature stored in the central server, so that the remote computer is protected from it without the need to wait for the latest signatures to be downloaded and installed on the remote computer. This technique can also give the advantage of moving the processing burden from the remote computer to the central server. However, this technique is limited by sending only signature information or very basic information about an object to the central server. Therefore, in order to analyse whether or not an unknown object is malware, a copy of that object is normally sent to the central server where it is investigated by a human analyst. This is a time consuming and laborious task introducing considerable delay in classifying malware as safe or unsafe. Also, given the considerable volume of new objects that can be seen daily across a community, it is unrealistic to have a skilled human analyst investigate each new object thoroughly. Accordingly, malevolent objects may escape investigation and detection for considerable periods of time during which time they can carry out their malevolent activity in the community.

We refer in the following to our previous application US-A-2007/0016953, published 18th January 2007, entitled "METHODS AND APPARATUS FOR DEALING WITH MALWARE", the entire contents of which are hereby incorporated by reference. In this document, various new and advantageous cloud-based strategies for fighting malware are disclosed. In particular a cloud based approach is outlined where the central server receives information about objects and their behaviour on remote computers throughout the community and builds a picture of objects and their behaviour seen throughout the community. This information is used to make comparisons with this

data across the community in developing and applying various heuristics and or rules to determine whether a newly seen object is malevolent or not.

This approach to fighting malware involves communicating, storing and managing vast amounts of data at the central server which is a challenging problem in itself. It is also challenging to develop new schemes for more accurately and more efficiently detecting malware given the vast amount of data collected about objects seen in the community and the constantly evolving strategies used by malware writers to evade detection. It is also desirable to improve the processes for analysing the data to make the best use of the time and specialised skills of the human malware analysts.

Malware is also becoming increasingly adept at self-defence by interfering with the operation of security programs installed on a computer. This is another problem that security software must contend with.

The present disclosure builds on the techniques disclosed in our previous application US-A-2007/0016953 to address these and other problems, as will become apparent in view of the following disclosure.

According to a first aspect of the present invention, there is provided a method of classifying a computer object as malware, the method comprising:

at a base computer, receiving data about a computer object from each of plural remote computers on which the object or similar objects are stored and or processed;

wherein the base computer comprises plural threat servers arranged to receive said data from the plural remote computers and apply rules and or heuristics against that data in real time to determine whether or not said object is malware and to communicate said determination to the remote computers;

said base computer further comprising at least one central server in communication with the threat servers and arranged to receive said data about objects from the threat servers to maintain a master database of data received about objects from all of the threat servers.

In the preferred embodiments, the threat servers make real time decisions as to whether or not an object is benign or malevolent based on the details of that object sent from the remote computers. Each threat server is connected to a database which contains entries for all of the objects known to the base computer and a classification of whether the object is safe or unsafe. The database may also store rules for deciding whether unknown objects are safe or unsafe based on the information received from the remote computer. The central server provides a master database of all data received about all objects. This can be used by human analysts or computer analysis in investigating malware threats.

Preferably, at least one threat server comprises at least one database for holding information received from remote computers to which it is attached, the method comprising: storing said data in at least one database at the threat server; and, at intervals, storing the contents of the database in storage together with a timestamp and the database. The intervals may be predetermined or dynamically set. This data structure has many advantages in providing secure, scalable, reliable updating of the data. This scheme reduces workload and traffic in the network by a significant factor compared with a conventional scheme where typically each piece of data on being received by a threat server would immediately be propagated to all other threat servers in the system that are to hold the data.

Preferably, the method comprises creating a backup central server by receiving at a central server all of the timestamped blocks of data and incorporating them into its database. Thus, backup servers can be quickly created with the current data set without interfering with the operation of current "live" servers. The live servers do not need to go off-line and can continue to function as the backup servers are created.

In an embodiment, the method comprises: taking a central server off-line for a period of time such that it does not receive updates of data from the threat servers during that period of time; after the period of time has elapsed, updating the database of the central server with timestamped blocks of data from the storage that have a timestamp later than the time when the central server went off-line; and, bringing the central server

back on line. This allows a central server to be taken offline, e.g. for maintenance or software updates, and updated quickly and simply so to have current data. No other server has to be taken off line or otherwise affected by this process.

In an embodiment, the method comprises rolling back the database of a central server to a point of time in the past; and, updating the database of the central server with timestamped blocks of data from storage that have a timestamp later than said past point of time; and, bringing the central server back on line. Thus, if the database is corrupted for any reason, the database can be rolled back to a point before the corruption happened. The database can then be updated with the missing data. Again, no other server is taken offline or otherwise affected by this process.

Preferably, the central server has databases including any one or more of: a) object signatures and metadata about that object; b) object behaviour; and, c) information about what objects are present on what remote computers. This allows the base computer to build up a full picture of the activities of objects and their attributes and behaviour across the community, allowing deep analysis to be performed to identify malware and trends and shifts in the data.

In a preferred embodiment, said threat and central servers are implemented using cloud computing. This allows "elastic" computing, such that the system administrators can create, launch, and terminate server instances as needed, paying only for what computing resources are used, and allows control over the geographical location of instances which allows for latency optimization and high levels of redundancy.

Preferably the method comprises: maintaining at a threat server, a list of objects previously seen at that threat server and forwarded to the central server; and, if an object has not been seen before, sending the data about that object to the central server, and if an object has been seen before, increasing the count for that object instead of sending the data. This reduces significantly the network traffic and load on the network and servers.

According to a second aspect of the present invention, there is provided apparatus for classifying a computer object as malware, the apparatus comprising:

a base computer arranged to receive data about a computer object from each of plural remote computers on which the object or similar objects are stored and or processed;

wherein the base computer comprises plural threat servers arranged to receive said data from the plural remote computers and apply rules and or heuristics against that data in real time to determine whether or not said object is malware and to communicate said determination to the remote computers;

said base computer further comprising at least one central server in communication with the threat servers and arranged to receive said data about objects from the threat servers to maintain a master database of data received about objects from all of the threat servers.

According to a third aspect of the present invention, there is provided a method of classifying a computer object as malware, the method comprising:

at a base computer, receiving data about a computer object from each of plural remote computers on which the object or similar objects are stored and or processed;

counting the number of times in a given time period objects having one or more common attributes or behaviours that have been seen by the remote computers;

comparing the counted number with the expected number based on past observations; and,

if the comparison exceeds some predetermined threshold, flagging the objects as unsafe or as suspicious.

As will be appreciated, the amount of data received from an agent program running on remote computers can be vast and therefore suited to being processed by computer. It would be impractical to have human operators look at all of this data to determine malware. This aspect allows greater focus to be placed on researching these outliers. Processes can be readily developed that can use this outlier information to automatically group, identify or prioritise research effort and even make malware determinations. Where automated rules are used to identify malware, this information

can be used to automatically heighten sensitivity of these rules when applied to objects in the group that has been identified as an outlier.

The attribute of the object may be one or any combination of: the file name, the file type, the file location, vendor information contained in the file, the file size, registry keys relating to that file, or any other system derived data, or event data relating to the object.

According to a fourth aspect of the present invention, there is provided apparatus for classifying a computer object as malware, the apparatus comprising a base computer arranged to receive data about a computer object from each of plural remote computers on which the object or similar objects are stored and or processed; the base computer being arranged to:

count the number of times in a given time period objects having one or more common attributes or behaviours that have been seen by the remote computers;

compare the counted number with the expected number based on past observations; and,

if the comparison exceeds some predetermined threshold, flag the objects as unsafe or as suspicious.

According to a fifth aspect of the present invention, there is provided a method of classifying a computer object as malware, the method comprising:

at a base computer, receiving data about a computer object from each of plural remote computers on which the object or similar objects are stored and or processed;

storing said data in a database; and,

presenting the user with a display of information relating to a group of plural objects and various attributes of those objects, the display being arranged such that commonality is shown between objects, wherein the group of objects displayed correspond to a user query of the database.

Thus, by being able to query and analyse the collective view of an object, i.e. its metadata and behaviours, across all remote computers that have seen it, a more informed

view can be derived, whether by human or computer, of the object. In addition it is possible to cross-group objects based on any of their criteria, i.e. metadata and behaviour.

The users employed in grouping objects according to this scheme need not be skilled malware analysts. The users need only basic training in use of the tool and in grouping objects by running queries and looking for commonality. The final analysis of objects covered by the query can be taken by a skilled malware analyst. A key advantage of this system is that the computer is doing the work in processing the raw data which is too large of a task to be practical for a human operator to complete. The human operators grouping the data need not be skilled, which reduces costs for the business. This reduces costs and leaves the skilled malware analysts to concentrate on queries that are found to be good candidates for further investigation. Thus, the skill of these operators is most effectively deployed in using their experience to identify malware.

In an embodiment, the information is displayed in tabular form with rows of the table corresponding to objects and columns of the table corresponding to attributes of the objects. Nonetheless, other forms of display can be used e.g. graphs, charts, 3D-visualiztions etc.

Preferably, at least one attribute of the objects is presented to the user pictorially such that objects with common attributes are given the same pictorial representation. In a preferred embodiment, the pictorial representation comprises symbols having different shapes and/or colours. This allows the user to spot commonality in the attribute at a glance. This works well for attributes where commonality is important and the actual value of the attribute is relatively unimportant.

Preferably, the method comprises: identifying commonality in one or more attributes between objects; and, refining the query in accordance with said identified commonality. By refining the query according to discovered commonality the user can quickly and simply investigate malware. The data grouped the queries can be flagged for

further investigation by a human analyst or be immediately flagged as benign or malevolent.

Preferably the method comprises creating a rule from a user query if it is determined that the query is deterministic in identifying malware.

In a preferred embodiment, the method comprises monitoring user groupings of objects along with any and all user actions taken such as classifying the objects of the group as being safe or unsafe; automatically applying said groupings and actions in generating new rules for classifying objects as malware. Thus, by tracking these actions it is possible for the server to learn from human analysts how to identify and determine objects automatically. The application can preferably remember queries that have been run by users. If the same query is being run repeatedly by a user and returning malware objects, or if a researcher consistently takes the action of determining the objects to be malware, then the system can automatically identify this condition and create a rule of the criteria and the action to determined matching objects as malicious.

Preferably, the method comprises applying the rule to an object at the base computer and or sending the rule to a remote computer and applying the rule to an object at the remote computer to classify the object as safe or unsafe. Thus, protection can be given in real time against previously unseen objects by applying the rules to the objects. Agent software running at the remote computer can apply the rules against objects for example in the event that contact with the base computer is lost allowing the agent software to carry on providing protection against new malware objects even when the base computer is "offline".

Preferably, the method comprises storing the classification of an object as safe or unsafe according to the rule in the database at the base computer. This information can taken into account in evaluating the performance of rules and in formulating new rules.

In a preferred embodiment, the method comprises receiving information from a remote computer that an object classified as malware by said rule is believed not to be

malware; and, amending or deleting the rule in accordance with said information. This allows feedback on the performance of the rule to the central server which can be taken into account in amending or deleting the rule if necessary and which may be taken into account in determining future rules.

According to a sixth aspect of the present invention, there is provided apparatus for classifying a computer object as malware, comprising a base computer arranged to receive data about a computer object from each of plural remote computers on which the object or similar objects are stored and or processed; the base computer being arranged to:

store said data in a database; and,

present the user with a display of information relating to a group of plural objects and various attributes of those objects, the display being arranged such that commonality is shown between objects, wherein the group of objects displayed correspond to a user query of the database.

According to a seventh aspect of the present invention, there is provided a method of operating a security program on a computer, comprising operating the security program to impersonate or use operating system functions in monitoring objects running on the computer, said monitoring being to determine whether the objects are malware.

This allows the program to resist attacks from malevolent objects. The program may perform operations by impersonating the system's context when it is necessary to rely on standard system calls, or circumventing any system calls by accessing data at the raw level as it is stored on disk. In doing so, the malware cannot react by killing the process as the process is the operating system. To kill the operating system would also prevent the malware from operating.

According to an eight aspect of the present invention, there is provided a computer program for fighting malware, the computer program comprising program instructions which when run on a computer cause the computer to monitor objects

running on the computer to determine whether the objects are malware or not, the monitoring being such that the program impersonates or uses operating system functions.

According to a ninth aspect of the present invention, there is provided a method of operating a security program on a computer, comprising:

loading a first component of the security program on the computer;

dynamically creating a second component of the security program on the computer having different attributes from the first component and which will automatically load in the event that the first component fails to load due to malevolent activity.

Preferably, the second component would have identical functionality but would be modified so as to appear different by name and form. In this scenario should the primary executable fail to load, most likely due to being killed by malware, the second component would be loaded to perform its function. If the primary executable loads successfully, the secondary executable would simply terminate to avoid conflict by identifying the presence of the primary executable.

Preferably the second component is arranged to remove its own digital signature.

According to a tenth aspect of the present invention, there is provided a computer program for fighting malware, the computer program comprising program instructions which when run on a computer program cause the computer to load a first component of the security program on the computer; and to dynamically create a second component of the security program on the computer having different attributes from the first component and which will automatically load in the event that the first component fails to load due to malevolent activity.

According to an eleventh aspect of the present invention, there is provided a computer program as described above recorded on a carrier.

According to a twelfth aspect of the present invention, there is provided a method of connecting a remote computer to one of a plurality of servers, the method comprising:

installing an agent program on the remote computer; the agent program having an algorithm for allocating the remote computer to a server determined by the time when the agent program was installed; and,

connecting the agent program to the allocated server.

The preferred embodiment provides a simple, pseudo random way of dynamically mapping remote computers to servers, which shares the load evenly between servers, even if several thousand remote computers are being installed simultaneously. This compares with some prior art schemes where dedicated hardware is used to share the load between servers.

Preferably the algorithm allocates the remote computer to a server determined also by the proximity of the remote computer to the servers. By allocating based on location, latency can be minimised.

Preferably the method comprises connecting the remote computer to the server using a DNS distribution network. This provides a convenient way of mapping server names to physical addresses of servers.

Preferably the agent program has a secondary algorithm to determine a secondary server for the remote computer in case the originally allocated server is inaccessible. This provides useful back up in case, for example, the originally allocated server is not operable, or if malware interferes with the mechanism, e.g. a DNS network, used to map servers to physical addresses. Preferably, the method comprises connecting the remote computer to a different server in accordance with information received by the agent program from the originally allocated server. These techniques allow more flexibility and centralised control to reallocate remote computers to servers.

According to a thirteenth aspect of the invention, there is provided a computer program comprising program instructions for:

allocating the remote computer to one of a plurality of servers determined by the time when the program was installed on the remote computer; and,

connecting the agent program to the allocated server.

According to a fourteenth aspect of the present invention, there is provided a computer program as described above recorded on a carrier. The carrier can be any physical medium, e.g. disk, USB storage, hard drive, optical media, etc.

According to a fifteenth aspect of the present invention, there is provided a method of providing protection against malware, the method comprising:

executing an agent program on a remote computer connected to a network, the agent program being configured to communicate with a base computer via the network, the agent program including a firewall arranged to block communications between the remote computer and entities on the network in accordance with predetermined rules; and,

configuring the firewall in accordance with rules received from the base computer.

The configurable firewall of the preferred embodiment can therefore leverage the rules and knowledge developed about malevolent objects and network URLs held at the base computer to provide a next line of defence in fighting malware by disabling the communications of the malware. In known firewalls, typically the user must manually configure the firewall.

Preferably, the method comprises: receiving at the remote computer from the base computer information that an object on the remote computer and or an entity on the network is unsafe; and, including a rule at the remote computer so that intended network communications involving the unsafe object and or unsafe entity are blocked by the firewall. The firewall can thus be configured to stop communications between a malevolent object on the remote computer trying to communicate with an entity on the network, such as a third party server, or stop communications between any object on the remote computer and a network location known to be associated with malevolent

activity, such as a URL operated by known criminals. This can be used to prevent, for example, criminals stealing personal data, passwords, etc.

Preferably the method comprises: receiving at the remote computer from the base computer information that an object on the remote computer and or an entity on the network is unsafe; asking permission from the user of the remote computer for details of intended network communications involving the unsafe object and or unsafe entity to be shared with a third party; and, intercepting intended network communications involving the unsafe object and or the unsafe entity and sharing them with a third party. This addresses the fact that in the prior art most of the effort in tackling cyber crime concentrates on stopping the effects of the malware, rather than identifying and trying to stop the criminals behind the malware. One difficulty is that it is illegal for the anti-malware or even the police to hack into the criminal's servers to find the criminal's data. Indeed, it a known ruse for the criminals to use so-called "botnets", which are "zombie networks" of legitimate users' computers which have been infected by malware and are thereby under the control of the criminals. The preferred embodiment keeps a record of communications involving malware, so the authorities can see what data was being stolen by the criminals. For legal reasons, the user's consent is obtained before sending any data to third parties. This can be implemented in various ways: 1) always ask (for every applicable detection), 2) obtain blanket permission per malware type, and 3) obtain blanket permission regardless of malware type.

According to a sixteenth aspect of the present invention, there is provided a computer program for providing protection against malware comprising program instructions which when executed on a remote computer connected to a network:

communicate with a base computer via the network, the computer program including a firewall arranged to block communications between the remote computer and entities on the network in accordance with predetermined rules; and,

configuring the firewall in accordance with rules received from the base computer.

As will become apparent in view of the following disclosure, the features of any

embodiment described above can be combined with any of the features of any other embodiment of any aspect of the invention as described above.

Embodiments of the present invention will now be described by way of example with reference to the accompanying drawings, in which:

Figure 1 shows schematically apparatus in which an embodiment of the present invention may be implemented;

Figure 2 is a flowchart showing schematically the operation of an example of a method according to an embodiment of the present invention;

Figure 3 shows a more detailed view of an example of a base computer 3 according to an embodiment of the present invention;

Figure 4 shows an example where web servers are located in different geographical locations;

Figure 5 shows schematically the apparatus of Figure 3 in more detail and in particular the way in which data can be moved from the FX layer to the ENZO layer in an embodiment;

Figure 6 shows schematically an example in which a new instance of an ENZO server is created in accordance with an embodiment of the invention;

Figure 7 shows schematically an example of apparatus by which an ENZO server shares out its workload between plural servers in accordance with an embodiment of the invention;

Figure 8 is a chart showing an example of a scheme for analysing data about objects according to an embodiment of the present invention;

Figure 9 show shows schematically an example of a scheme for processing data about objects according to an embodiment of the invention;

Figures 10 to 13 show graphical user interfaces of an example of a computer program for researching objects according to an embodiment of the present invention;

Figure 14 shows an example of an agent program on a remote computer according to an embodiment of the present invention; and,

Figure 15 shows the hierarchy on a computer system.

OVERVIEW

Referring to Figure 1, a computer network is generally shown as being based around a distributed network such as the Internet 1. The present invention may however be implemented across or use other types of network, such as a LAN. Plural local or "remote" computers 2 are connected via the Internet 1 to a "central" or "base" computer 3. The computers 2 may each be variously a personal computer, a server of any type, a PDA, mobile phone, an interactive television, or any other device capable of loading and operating computer objects. An object in this sense may be a computer file, part of a file or a sub-program, macro, web page or any other piece of code to be operated by or on the computer, or any other event whether executed, emulated, simulated or interpreted. An object 4 is shown schematically in the figure and may for example be downloaded to a remote computer 2 via the Internet 1 as shown by lines 5 or applied directly as shown by line 6. The object 4 may reside in computer RAM, on the hard disk drive of the computer, on removable storage connected to the computer, such as a USB pen drive, an email attachment, etc.

In one preferred embodiment, the base computer 3 is in communication with a database 7 with which the remote computers 2 can interact when the remote computers 2 run an object 4 to determine whether the object 4 is safe or unsafe. The community

database 7 is populated, over time, with information relating to each object run on all of the connected remote computers 2. As will be discussed further below, data representative of each object 4 preferably takes the form of a so-called signature or key relating to the object, its attributes and behaviour.

Referring now to Figure 2, at the start point 21, a computer object 4 such as a process is run at a remote computer 2. At step 22, by operation of a local "agent" program or software running on the remote computer 2, the operation of the process is hooked so that the agent program can search a local database stored at the remote computer 2 to search for a signature or key representing that particular process, its related objects and/or the event. If the local signature is present, it will indicate either that the process is considered to be safe or will indicate that that process is considered unsafe. An unsafe process might be one that has been found to be malware or to have unforeseen or known unsafe or malevolent results arising from its running. If the signature indicates that the process is safe, then that process or event is allowed by the local agent program on the remote computer 2 to run at step 23. If the signature indicates that the process is not safe, then the process or event is stopped at step 24.

It will be understood that there may be more than two states than "safe" or "not-safe" and choices may be given to the user. For example, if an object is considered locally to be not safe, the user may be presented with an option to allow the related process to run nevertheless. It is also possible for different states to be presented to each remote computer 2. The state can be varied by the base computer to take account of the location, status or ownership of the remote computer or timeframe.

Furthermore, the agent software at the remote computer 2 may be arranged to receive rules or heuristics from the base computer 3 for classifying objects as safe or unsafe. If the object is unknown locally, the agent software may apply the rules or heuristics to the details of the object to try to classify the object as safe or unsafe. If a classification is made, details of the object and classification are passed to the base computer 3 to be stored in the community database 7. This means that the agent software is capable of providing protection against previously unseen objects even if it is

"offline", e.g. it is unable to connect to the base computer for any reason. This mechanism is described in more detail later in the disclosure.

If the object is still not classified locally, then details of the object are passed over the Internet 1 or other network to the base computer 3 for storing in the community database 7 and preferably for further analysis at the base computer 3. In that case, the community database 7 is then searched at step 25 for a signature for that object that has already been stored in the community database 7. The community database 7 is supplied with signatures representative of objects, such as programs or processes, run by each monitored remote computer 2. In a typical implementation in the field, there may be several thousands or even millions of remote computers 2 connected or connectable to the base computer 3 and so any objects that are newly released upon the Internet 1 or that otherwise are found on any of these remote computers 2 will soon be found and signatures created and sent to the base computer 3 by the respective remote computers 2.

When the community database 7 is searched for the signature of the object that was not previously known at the remote computer 2 concerned, then if the signature is found and indicates that that object is safe, then a copy of the signature or at least a message that the object is safe is sent to the local database of the remote computer 2 concerned at step 26 to populate the local database. In this way, the remote computer 2 has this information immediately to hand the next time the object 4 is encountered. A separate message is also passed back to the remote computer 2 to allow the object to run in the current instance.

If the signature is found in the community database 7 and this indicates for some reason that the object is unsafe, then again the signature is copied back to the local database and marked "unsafe" at step 27, and/or a message is sent to the remote computer 2 so that running of the object is stopped (or it is not allowed to run) and/or the user given an informed choice whether to run it or not.

If after the entire community database 7 has been searched the object is still unknown, then it is assumed that this is an entirely new object which has never been seen

before in the field. A signature is therefore created representative of the object at step 28, or a signature sent by the remote computer 2 is used for this purpose.

At this point, rules or heuristics may be applied by the base computer 3 to the details of the object to try to classify the object as safe or unsafe. If a classification is made, the signature is marked as safe or unsafe accordingly in the community database 7. The signature is copied to the local database of the remote computer 2 that first ran the object. This mechanism is described in more detail later in the disclosure.

If the object is still not classified, the signature may be initially marked as bad or unsafe in the community database 7 at step 29. The signature is copied to the local database of the remote computer 2 that first ran the object at step 30. A message may then be passed to the remote computer 2 to instruct the remote computer 2 not to run the object or alternatively the user may be given informed consent as to whether to allow the object to run or not. In addition, a copy of the object itself may be requested at step 31 by the community database 7 from the remote computer 2.

If the user at the remote computer 2 chooses to run a process that is considered unsafe because it is too new, then that process may be monitored by the remote computer 2 and/or community database 7 and, if no ill effect occurs or is exhibited after a period of time of n days for example, it may then be considered to be safe. Alternatively, the community database 7 may keep a log of each instance of the process which is found by the many remote computers 2 forming part of the network and after a particular number of instances have been recorded, possibly with another particular number of instances or the process being allowed to run and running safely, the signature in the community database 7 may then be marked as safe rather than unsafe. Many other variations of monitoring safety may be done within this concept.

The database 7 may further include a behaviour mask for the object 4 that sets out the parameters of the object's performance and operation. If an object is allowed to run on a remote computer 2, even if the initial signature search 22 indicates that the object is safe, then operation of that object may be monitored within the parameters of the mask.

Any behaviour that extends beyond that permitted by the mask is identified and can be used to continually assess whether the object continues to be safe or not.

The details of an object 4 that are passed to the base computer 3 are preferably in the form of a signature or "key" that uniquely identifies the object 4. This is mainly to keep the data storage and transmission requirements as minimal as possible. This key may be formed by a hashing function operating on the object at the remote computer 2.

The key in the preferred embodiment is specially arranged to have at least three severable components, a first of said components representing executable instructions contained within or constituted by the object, a second of said components representing data about said object, and a third of said components representing the physical size of the object. The data about the object in the second component may be any or all of the other forms of identity such as the file's name, its physical and folder location on disk, its original file name, its creation and modification dates, resource information such as vendor, product and version, and any other information stored within the object, its file header or header held by the remote computer 2 about it; and, events initiated by or involving the object when the object is created, configured or runs on the respective remote computers. In general, the information provided in the key may include at least one of these elements or any two or more of these elements in any combination.

In one preferred embodiment, a checksum is created for all executable files, such as (but not limited to) .exe and .dll files, which are of the type PE (Portable Executable file as defined by Microsoft). Three types of checksums are generated depending on the nature of the file:

Type 1: five different sections of the file are check summed. These include the import table, a section at the beginning and a section at the end of the code section, and a section at the beginning and a section at the end of the entire file. This type applies to the vast majority of files that are analysed;

Type 2: for old DOS or 16 bit executable files, the entire file is check summed;

Type 3: for files over a certain predefined size, the file is sampled into chunks which are then check summed. For files less than a certain predefined size, the whole file is check summed.

For the check summing process, in principle any technique is possible. The MD5 (Message-Digest algorithm 5) is a widely-used cryptographic hash function that may be used for this purpose.

This allows a core checksum to be generated by viewing only the executable elements of the checksum and making a comparison between two executables that share common executable code.

For the type 1 checksum mentioned above, three signature processes may be used. The first defines the entire file and will change with almost any change to the file's content. In particular, the first defines a representative sampling of the contents of the program in that if any fundamental change is made to the program, the checksum will change, but trivial changes can be identified as such, allowing correlation back to the original program body. The second attempts to define only the processing instructions of the process which changes much less. The third utilises the file's size, which massively reduces the potential of collisions for objects of differing sizes. By tracking the occurrences of all signatures individually appearing with different counterparts, it is possible to identify processes that have been changed or have been created from a common point but that have been edited to perform new, possibly malevolent functionality.

As well as checksum data, metadata about the object is preferably captured and sent to the base computer 3. Amongst other types, the types of metadata captured and sent to the base computer 3 might be:

"Events": these define the actions or behaviours of an object acting upon another object or some other entity. The event has three principal components: the key of the

object performing the act (the "Actor"), the act being performed (the "Event Type"), and the key of the object or identity of another entity upon which the act is being performed (the "Victim"). For example, the event data might capture the identity, e.g. the IP address or URL, of a network entity with which an object is communicating, another program acting on the object or being acted on by the object, a database or IP registry entry being written to by the object, etc. While simple, this structure allows a limitless series of behaviours and relationships to be defined. Examples of the three components of an event might be:

Actor	Event Type	Victim
Object 1	Creates Program	Object 2
Object 1	Sends data	IP Address 3
Object 1	Deletes Program	Object 4
Object 1	Executes	Object 2
Object 2	Creates registry key	Object 4

"Identities": these define the attributes of an object. They include items such as the file's name, its physical location on the disk or in memory, its logical location on the disk within the file system (its path), the file's header details which include when the file was created, when it was last accessed, when it was last modified, the information stored as the vendor, the product it is part of and the version number of the file and it contents, its original file name, and its file size.

"Genesisactor": the key of an object that is not the direct Actor of an event but which is the ultimate parent of the event being performed. For example in the case of a software installation, this would be the key of the object that the user or system first executed and that initiated the software installation process, e.g. Setup.exe.

"Ancillary data": many events may require ancillary data, for example an event such as that used to record the creation of a registry run key. In this situation the "event" would identify the Actor object creating the registry run key, the event type itself (e.g.

"regrunkey"), and the Victim or subject of the registry run key. The ancillary data in this case would define the run key entry itself; the Hive, Key name and Value.

"Event Checksums": because the event data can be quite large extending to several hundred bytes of information for a single event, its identities for the Actor and Victim and any ancillary data, the system allows for this data itself to be summarised by the Event Checksums. Two event checksums are used utilising a variety of algorithms, such as CRC and Adler. The checksums are of the core data for an event. This allows the remote computer 2 to send the checksums of the data to the central computer 3 which may already have the data relating to those checksums stored. In this case, it does not require further information from the remote computer 2. Only if the central computer 3 has never received the checksums will it request the associated data from the remote computer 2. This affords a considerable improvement in performance for both the remote and central computers 2,3 allowing much more effective scaling.

Thus, the metadata derived from the remote computers 2 can be used at the community database 7 to define the behaviour of a process across the community. As mentioned, the data may include at least one of the elements mentioned above (file size, location, etc.) or two or three or four or five or six or all seven (or more elements not specifically mentioned here). The data stored in the community database 7 provides an extensive corollary of an object's creation, configuration, execution, behaviour, identities and relationships to other objects or entities that either act upon it or are acted upon by it. This may be used accordingly to model, test and create new automated rules and heuristics for use in the community database 7 and as rules that may be added to those held and used in the local database of the remote computers 2 to identify and determine the response of the remote computers 2 to new or unknown processes and process activity.

Moreover, it is possible to monitor a process along with any optional sub-processes as a homogenous entity and then compare the activities of the top level process throughout the community and deduce that certain, potentially malevolent practices only occur when one or more specific sub-processes are also loaded. This allows effective

monitoring (without unnecessary blocking) of programs, such as Internet Explorer or other browsers, whose functionality may be easily altered by downloadable optional code that users acquire from the Internet, which is of course the principal source of malevolent code today.

DISTRIBUTED ARCHITECTURE

The system as described so far is generally as described in our previous application US-A-2007/0016953. There now follows a description of new, advantageous schemes in operating such a system. It will be appreciated that in the description in relation to Figures 1 and 2 the central computer and the community database are presented for convenience as single entities. As will be apparent from the following discussion, the base computer 3 can be comprised of multiple computers and servers, etc. and the community database 7 can be made up multiple databases and storage distributed around this central system.

Figure 3 shows a preferred example of an arrangement for the base computer 3. The remote computer 2 has an agent program 10 which generally includes the same functionality as the agent program described above in relation to Figures 1 and 2. In short, the agent program 10 the monitors objects on that computer 2 and their behaviour and communicates with the base computer 3 to send details of new objects and behaviour found on the remote computer 2 and to receive determinations of whether the objects are safe or not. The agent program 10 optionally communicates with a local database 11 which holds a local copy of signatures relating to the objects found on the remote computer 2.

The agent program 10 can be comparatively small compared with other commercially available anti-malware software. The download size for the agent program 10 can be less than 1 MB and occupy about 3 MB of memory when running, using more memory only to temporarily hold an image of a file(s) being scanned. In comparison, other anti-malware packages will typically have a download of 50 MB and

occupy 50 MB to 200 MB of computer memory whilst scanning files. Thus, the preferred architecture can occupy less that 2% of system resources compared with other products.

This is achieved primarily by the preferred agent program 10 being developed in a low-level language, having direct access to system resources such as the video display, disk, memory, the network(s), and without the incorporation of many standard code or dynamic linked libraries to perform these functions. Memory usage is optimised by storing data in the local database structure that provides the ability to refer to objects by a unique identifier rather than requiring full filenames or signatures. All unnecessary dynamic link libraries are unloaded from the process immediately as they are identified as no longer being used, and background threads are merged to reduce CPU usage. A small, efficient agent can be deployed more quickly and can used alongside other programs, including other security programs, with less load on or impact on the computer's performance. This approach also has the advantage of having less surface area for attack by malware making it inherently more secure.

The agent program 10 communicates with the base computer 3 over the Internet 1 via the Internet's Domain Name Resolution System (DNS) 50.

The base computer 3 has a first layer comprising one or more servers 61, which in this example are web servers. In the present disclosure, the web servers 61 are referred to as "FX servers" or "threat servers" and the first layer is referred to as the "FX layer". However, it will be appreciated that any type of suitable server may be used according to need. The remote computers 2 are allocated to one of the web servers 61 as explained in more detail below.

The FX layer 60 makes real time decisions as to whether or not an object is benign or malevolent based on the details of that object sent from the remote computer 2. Each web server 61 of the FX layer 60 is connected to a database 62 which contains entries for all of the objects known to the base computer 3 and a classification of whether the object is safe or unsafe. The database 62 also stores rules for deciding whether

unknown objects are safe or unsafe based on the information received from the remote computer 2. The web server 61 first searches the database 62 for matching signatures to determine if the object is safe or unsafe or unknown. As described above, the signature can be a function of the hashes (checksum data) derived from file itself, event data involving the object and or metadata about the object in any combination. If the object is unknown, the web server 61 then determines if any of the rules classify the object as unsafe. The web server 61 then communicates back to the remote computer 2 whether the object is safe and can be allowed to run, unsafe and is to be prevented from running, or unknown in which case the object can be allowed to run or not according to user preference.

Thus, the FX layer 60 reacts in real time to threats to determine whether or not malware should be allowed to run on a remote computer 2.

Sitting behind the FX layer 60 is a second layer (called the "ENZO layer" 70 herein). Information about objects received by the FX layer 60 from the remote computers 2 is sent to the ENZO layer 70 such that a master record is maintained at the ENZO layer 70 of all data received from all remote computers 2. This process is described in more detail below.

The ENZO layer 70 has one or more servers 74 (referred to as “central servers” or “ENZO servers” in this disclosure) connected to one or more "master" databases which aggregate all of the information received from all web servers 61 from all remote computers 2. The databases may comprise any combination of the following three databases and in the preferred embodiment has all three.

1) An object database 71, which has entries containing object signatures (e.g. their MD5 checksums) and including metadata received about objects, e.g. file name, file location, or any other metadata collected by the system as described above.

2) A behaviour database 72 for capturing details of the behaviour of objects observed on a remote computer 2. This database 72 is populated by the event data sent from the

remote computers 2 and allows a picture to be built up of the behaviour and relationships an object has across the community.

3) A computer-object database 73 which associates remote computers 2 in the community with objects observed on those remote computers 2 by associating objects with identification codes sent from the remote computer 2 during object detail transmission. Preferably the computer is identified by at least the following three identifiers sent from the remote computer: one which relates to the physical system, one which relates to the operating system instance and one which relates to the logged on user.

As will be appreciated, in a community having for example 10 million or more remote computers 2, each having on average hundreds to thousands of objects, each having a large number of behaviours and associations with other objects, the amount of data held in the databases 71,72,73 is enormous.

The ENZO servers 74 can query the databases 71,72,73 and are operable, either by automation or by input from a human analyst or both, in monitoring object behaviour across the community and in investigating objects and developing rules for spotting malware. These rules are fed back to the FX layer 60 and or the agent program 10 running on remote computers 10 and, as discussed elsewhere in this document, are used by the web servers 61 or the agent program 10 in real time to stop malware from running on remote computers 2. The performance of those rules in accurately stopping malware on the remote computers 2 is fed back to the ENZO layer 70 and can be used to refine the rules. The techniques used are described further in the following disclosure.

In a preferred embodiment, some or all of the servers 61,74 and databases 62,71,72,73 of the FX and ENZO layers 60,70 are implemented using cloud computing. Cloud computing is a means of providing location-independent computing, whereby shared servers provide resources, software, and data to computers and other devices on demand. Generally, cloud computing customers do not own the physical infrastructure, instead avoiding capital expenditure by renting usage from a third-party provider. Cloud

computing users avoid capital expenditure on hardware, software, and services when they pay a provider only for what they use. New resources can quickly be put on line. This provides a large degree of flexibility for the user.

An example of cloud computing is the Amazon Elastic Compute Cloud (EC2) which is a central part of the Amazon.com cloud computing platform, Amazon Web Services (AWS). Another example is the Windows Azure Platform which is a Microsoft cloud platform that enables customers to deploy applications and data into the cloud. EC2 is used in the present example to provide cloud computing. Nonetheless, it will be appreciated that, in principle, any suitable cloud architecture could be used to implement the base computer 3. Alternatively conventional data centres could be used to implement the base computer 3, or a mixture of conventional data centres and cloud based architecture could be used.

EC2 allows users to rent virtual computers on which to run their own computer applications. EC2 allows scalable deployment of applications by providing a web service through which a user can boot an Amazon Machine Image to create a virtual machine, which Amazon calls an "instance", containing any software desired.

A user can create, launch, and terminate server instances as needed, paying by the hour for active servers, allowing the provision of "elastic" computing. EC2 provides users with control over the geographical location of instances which allows for latency optimization and high levels of redundancy. For example, to minimize downtime, a user can set up server instances in multiple zones which are insulated from each other for most causes of failure such that one backs up the other. In this way, the cloud provides complete control of a user's computing resources and its configuration, i.e. the operating system and software packages installed on the resource. Amazon EC2 allows the user to select a configuration of memory, CPU, instance storage, and the boot partition size that is optimal for the operating system and application. EC2 reduces the time required to obtain and boot new server instances to minutes, allowing the user to quickly scale capacity, both up and down, their computing requirements change.

EC2 maintains a number of data centres in different geographical regions, including: US East Coast, US West Coast, EU (Ireland), and Asia Pacific (APAC) (Singapore). As shown by Figure 4, in a preferred embodiment, the servers and databases of the base computer 3 are implemented in plural of these geographical locations 80.

The important question therefore arises of how to allocate remote computers 2 to a particular instance of web server 61 in the FX layer 60. Important considerations in this decision are to minimise latency and to share the load evenly across the web servers. Ideally, the load on resources would be shared approximately equally across all instances of web servers in order to avoid web servers being under utilised and to minimise the number of web servers required. It is also desirable to implement a simple solution which does not add significantly to the speed or size of the agent program 10 on the remote computers, or place an overhead on the base computer 3.

1) In a preferred embodiment, the agent program 10 uses the geographical location of the remote computer 2 in allocating the remote computer 2 to a web server 61, i.e. based on its proximity to a geographical region 80 of the cloud. The location of the remote computer can be determined by any convenient means, such as examining the IP address of the remote computer 2 against a database of known location ranges, or performing a network route analysis to determine the number of "hops" required to reach the destination server. This functionality can be performed by the agent program 10 running on the remote computer 2 when it is first installed on the computer 2. By allocating based on location, latency can be minimised.

2) In a preferred embodiment, the agent program 10 generates a random number based on the date and time of its installation seeded with unique identifiers of the remote computer to decide to which web server 61 it should be mapped. This provides a simple, pseudo random way of mapping remote computers 2 to web servers 61 which shares the load evenly between web servers 61 even if several thousand remote computers are being installed simultaneously.

3) The DNS distribution layer then maps the URL to the physical data centre. The Domain Name System (DNS) is a hierarchical naming system built on a distributed database for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. The DNS distribution network 50 allows load balancing to plural servers 61 making up the FX layer 60.

Any combination of these techniques can be used by the agent program 10 to allocate a remote computer 2 to a web server 61. Preferably, all three are used in combination.

The agent program 10 preferably has a secondary algorithm to re-map the remote computer 2 to different URL in case the primary URL is unavailable for any reason, e.g. if the servers go down. Also, in the event that malware has been able to disable the DNS mechanism then the agent program 10 can make direct contact with the FX servers 61 by referring directly to a series of direct IP addresses reserved for this purpose.

Optionally, the agent program 10 is arranged so that it can reassign the remote computer 2 to a different server 61 by receiving feedback/instruction from the server 61 the computer is already connected to. This can be used to add central control to the allocation of agent program 10 to servers 61, which adds more flexibility to the system.

Thus, this scheme allows a simple, agent managed way of dynamically load balancing between servers and providing resiliency, whilst dealing with geographical location. In known prior art arrangements, specialised hardware load balancers are employed in the network to divide load to other servers, or else agents are manually allocated to web servers 61 when the agent program 10 is installed.

Using a cloud-based distributed architecture for the base computer 3 presents challenges in trying to maintain integrity of data across the servers and in managing the update of data across the many servers. As will be clear from the foregoing, the web servers 61 in a typical implementation will be dealing with huge amounts of data. There

will be large amounts of commonality in the data which can be used for determining rules on what objects are malware. However, it is impractical to store all data on all web servers 61 on all regions. This presents a problem in determining whether or not the data is common in real time.

To address these issues, a preferred embodiment adopts the following scheme. Each web server 61 in the FX layer 60 examines an incoming packet of data from a remote computer 2 about an object seen on that remote computer 2. The agent program 10 generates a checksum of the data packet and sends it to the web server 61. The web server 61 has a database 62 of objects that have previously been seen and which have already been sent to the ENZO server 74. The web server 61 checks its database 62 for the checksum of the incoming data. If the checksum is found, then the data has already been seen by the ENZO server 74. In this case, the web server 61 just increases the count associated with that checksum in its database of the number of times that data has been seen to assist in determining the popularity of a piece of software or the frequency of the occurrence of a specific event. This information can then be forwarded to the ENZO server 74. If the checksum is not found in the FX database 62, then the web server requests the full data packet from the remote computer and then forwards this to the ENZO server 74. The ENZO server 74 then stores this data in the appropriate databases 71,72,73. Thus, the ENZO layer 70 keeps a master list in the object database 71 of all data objects, their metadata and behaviour seen on all of the remote computers 2. This master list is propagated back to all of the web servers 61 in all of the geographical locations 80. Thus, all web servers 61 are updated with information about which objects have been seen by the community.

This scheme has been found to reduce workload and traffic in the network by a factor of about 50 compared with a conventional scheme where typically each piece of data on being received by a web server would immediately be propagated to all other servers in the system.

It is desirable that the data held in the master databases 71,72,73 in the ENZO layer 70 provide scalability, accessibility and resilience to the data for users. It will be

appreciated that if just one live ENZO server 74 is used, then if that server becomes inaccessible, all live data is lost. For this reason, it is preferred to have at least one ENZO server 74 in each region 80 of the cloud to provide redundancy. This means that the web servers 61 are not all directly linked to the same ENZO server 74, but rather the web servers 61 are only linked to the ENZO server 74 in their own region 80. This creates a need for an extensible method of providing data to multiple database servers.

Figure 5 shows schematically a scheme of updating data from a web server 61 to an ENZO server 74. Each web server 61 has two temporary databases 63a,63b linked to it. At an initial starting point, one database 63a is part full 63b (active) and the other is empty (inactive). As information about objects is received from a remote computer 2 by the web server 61, it posts the information into the active database 63a. This information will be checksum information received from the remote computers 2 about objects or events seen on the remote computer. If the checksum is previously unseen at the web server, the associated data about that object or event is posted to the database along with its checksum.

Once the active database 63a reaches a predetermined size or some other predetermined criteria is met, the contents of the active database 63a are put into long term storage 66 together with a time stamp of the point in time when this happens. While this is occurring, the inactive database 63b is made active and starts to fill with new data as it arrives, and the formerly active database 63a is cleared and made inactive. Again, when this database is full, then the process of time stamping and moving the contents of the database to long term storage is repeated and the databases are swapped over. In the preferred embodiment, the FX layer 60 has a S3 sub-layer 65 which is responsible for managing input/output to the long term storage 66. S3 (Simple Storage Service) is an online storage web service offered by Amazon Web Services. S3 is an Amazon service for the storage of high volume data in a secure and non volatile environment through a simple web services interface. S3 is used to store the history of the FX server data being sent from the FX servers to the ENZO servers. When a block of data is put into long term storage 66, the S3 layer 66 also forwards this data to the ENZO server 74 or servers so that the ENZO server can update its databases. All FX

servers feed all ENZO servers via the S3 storage service.

The databases 63a,63b may be emptied into long term storage 66 for example every few minutes or even every few seconds. However, as will be appreciated, the actual time period used can be selected according to the load and size of the databases and may be chosen dynamically based on for example the load on the database or the size of the data.

Thus, the S3 layer 65 holds all of the data received by all of the web servers 61 in the community. This has a number of advantages as illustrated by Figure 6.

Firstly, this can be used to allow the master ENZO databases 71,72,73 to be rebuilt for example in the event that an ENZO server 74 develops a problem. Also, if the data held by an ENZO server 74 is corrupted somehow, for example by a problem in a software upgrade on the ENZO server 74, it is possible to roll back the databases at the ENZO server 74 to a point before the corruption occurred. By using the timestamps associated with the blocks of data in the S3 layer 65, the ENZO server 74 can request the data blocks in long term storage 66 at the S3 layer 65 to be resent to the ENZO server 74 so the server's databases 71,72,73 can be brought up to date.

Furthermore, using this scheme, the ENZO servers 74 in multiple regions 80 can create backup databases of the ENZO databases by receiving the data from the S3 layer. This can be done without affecting the live ENZO databases 74, so these can carry on functioning seamlessly.

The alternative would be to post to databases at a single ENZO server which is designated the master server and to propagate the data from the master server to other servers in the community. However, this in effect creates one “live” server and one or more backups. The live server therefore does most of the work, e.g. pre-processing data received from the agents, updating the databases and analysing the data for threats, whilst the backup servers are under utilised. Thus, the live server must be more powerful than the backup servers. This tends to be wasteful and inefficient of resources. In

comparison, the preferred embodiment, shares the workload around the servers equally.

It is also desirable for operators, human malware analysts, etc, to have a copy of the data from a live server for research, etc. Image servers may be created in the same way as the live servers and the backup servers. The user of the system can take the image server offline when he needs to take an image for offline use. Once the image is taken, the image database can be brought up to date using the blocks of data from the S3 layer.

Cloud computing can recreate instances of web servers very quickly, e.g. in a matter of minutes. Cloud computing is therefore advantageous in implementations where the volume of transactions grows (or shrinks). In this situation, a new server instance can be quickly created to handle the new load. However, it is necessary to take an image of a live server to create the image. This is disruptive to the processes running on that instance during imaging. It is therefore clearly not acceptable to take a live server out of commission for this period. Therefore a special dedicated image server is maintained behind the ENZO server which is updated in a similar way to the live and backup servers. In this case, the image server is taken off-line and imaged. This process might take for example 30 minutes. During this time, the image server is not receiving updates from the S3 server and therefore becomes out of date. However, since the exact time when the server went off line is known, it can be updated by requesting data blocks from the S3 server with a timestamp later than when it went off line. Thus, an image can be taken of an updated server for offline use etc and brought back up to date without affecting the running of the system.

It is also desirable to be able to scale out the architecture of the ENZO layer 70. For example, a live server 74 may be running out of processing power due to the increase in traffic it is seeing from web servers 61 or agents 10. For example, more remote computers 2 may be connected to the system, or a common software package may be updated leading to a large volume of new data being sent to the ENZO layer 70. In this situation, a second or further live server instance can be created in the ENZO layer 70 in order to scale out horizontally (as opposed to adding more CPU/RAM to an existing

server). As described above, it is relatively straightforward to create an image of an ENZO server 74 in a cloud computing environment. As can be seen from Figure 7, the data on each server 74 is divided into a plurality of sections. In this case the data on the server 74 is divided into eight sections 0-7. Each section does a share of the processing on that server. When the server is divided, various sections are allocated to each server. So, for example, in the example of Figure 7, the original server L1 processes data 0-3, and the newly created server L2 processes data 4-7. Each server then handles pre-processing and storing its own data. For the purposes of analysing the data, the data from these multiple severs 74 is preferably aggregated by the servers so that the human analyst is working on the complete set of data when investigating malware (as described in more detail below). Of course, the data can be divided in different ways among the servers according to need.

So, instead of holding a single database and then having to dissect it if it is required to distribute the load across multiple servers, in the preferred embodiment the database is already dissected making it is much easier to make a transition to further distribution of the database workload across multiple servers.

The number of data sections is preferably selected to be eight, because this is enough to give reasonable flexibility and ability to expand. However, it is rare that a business needs to expand by more than 800% at any time. Nonetheless, other plural numbers of data sections can be used as appropriate.

This architecture allows vast amounts of data to be managed across multiple locations and servers. The architecture can be scaled and servers copied without incurring extra work or affecting the running of the system. The data can be exchanged across servers that can change dynamically.

USING TREND DATA

Malware evolves at a significant pace. Historically, malware used a single

infection (module or program) to infect many computers. As this allowed malware researchers to quickly become aware of the infection, signatures could be quickly deployed to identify and block the threat. In the last decade, malware authors have made their threats contain many varied modules which shared a common purpose. To detect and block these threats is a much greater challenge for malware research and to creating and distributing signatures to identify and block all of the variations, any one of which could infect one or more computers. Due to the varied and distributed nature of these modern threats malware researchers are often late in identifying that a threat even exists.

By collecting hashes, signatures and statistics of new programs and modules correlated by path and file details, and aggregating this information at a central location, it is possible to use a method of analysis that will allow faster identification of new threats.

On any given day the amount of new commercial programs and modules that are created can be considered almost constant. This data can be measured against any of the metadata or event data collected about the object. In one example, the data is measured against the Path (Folder) location of new files created. The data can also be measured against their filenames, and file types (e.g. .exe, .dll, .drv, etc.) along with details such as vendor, product and version information, registry keys, or any other system derived data forwarded to base computer. Any combination of these factors is possible. In whichever way it is chosen to group the data, by establishing a baseline for the pattern and distribution of this data across the groups it is possible to quickly identify outliers.

Figure 8 shows an example of collected data over a time period grouped according to folders in the file system compared with the established normal distribution (base line). If the number of new programs in the windows system32 subfolder is normally x in any given time period t (e.g. in a given day) and in a particular time period t1 under consideration it is 1.4x (or exceeds some other predetermined ratio) then it indicates an abnormal increase in the number of new files which signifies possible malware activity. This identification allows greater focus to be placed on researching these outliers. Processes can be readily developed that can use this outlier information to

automatically group, identify or prioritise research effort and even make malware determinations. Where automated rules are used to identify malware, this information can be used to automatically heighten sensitivity of these rules when applied to objects in the group that has been identified as an outlier.

Another example of this technique is to focus on a filename and compare the number of new objects (as represented by its hash) that utilize that name, or the number of new objects all of which have new names. This is contrary to the general principles of most commercial software which needs consistency to enable manageability of their products. Most commercial applications have only a few names and each file name has only a few variants as each new release is made available. In contrast, some malware has thousands of variants using the same, similar or similarly structured name and which are observed by the community utilising the related names within a very short window of time (seconds-weeks).

In principle, any length of time for the window can be selected. In practice, this is likely to be of the order of every 15 minutes, or every few hours, or a day, rather than longer periods like every week.

In a preferred embodiment, techniques are provided to provide context for researchers. In detecting malware, human analysts and computer automated analysis have different strengths and are often used together to some degree to harness the capabilities of both. Computers are good at applying rules to and processing large amounts of data. In the present application, the amount of data received from agent program 10 running on remote computers 2 is vast and therefore suited to being processed by computer. It would be impractical to have human operators to look at all of this data to determine malware. On the other hand, experienced human analysts are highly adept at spotting malware given the appropriately focussed data about that object and similar objects and their context. Often a human analyst can "intuitively" spot malware, in a way that is difficult to reduce to a set of rules and teach to a machine. For example, kernel32.dll is a file associated with the Windows (RTM) operating system. A malware program may be called something similar, e.g. kernel64.dll, which would

immediately be apparent to a user as being suspicious, but which it would be difficult to teach a machine to spot.

The pattern may be obvious in retrospect when an analyst is presented with the relevant data. However, this is a rear view mirror approach. The problem is finding the relevant data in the vast amount of data being received at the base computer 3 so that the analyst can focus his/her time on the important data. As illustrated by Figure 9, what is needed is some what of distilling the raw data 100 into groups of related data 101 to provide a focussed starting point for a malware researcher to investigate and take necessary action 102 to flag objects bad or safe 103 accordingly.

As will be appreciated, a single object on a remote computer 2 across the community can have a high degree of associations with other objects on remote computers 2. Some tools currently exist which can map links between entities to create a network of associations. However, when used for a malware object and its associations with other objects, these will result in a diagram that is so dense and complicated that it is practically useless for the purpose of allowing a human analyst to identify malware. The problem is sifting this data so useful features are extracted for the analyst so that he can quickly focus on the likely candidates for being malware.

A preferred embodiment, illustrated by Figures 10 to 13, provides a software program running on the ENZO server 74 and giving the user a visual based tool for running queries against the databases. A query language such as TSQL may be used for example to query the database based on the user's input. As mentioned in the foregoing, the ENZO layer 70 has a complete record of the properties and activities of all objects seen on all remote computers 2 in their databases. Figure 10 shows an example of an on screen display and user interface including a table 105 in which the rows represent the objects (determined by their signatures) that match the results of the current query. The user interface provides tools for creating new queries 106, for displaying current and recent queries 107 and for sorting the data displayed in the table for the current query 108. Clearly there may be more results than will fit on one screen. There may therefore be more than one page of results to which the user can navigate through appropriate

controls 109 provided by the user interface.

The table 105 has a plurality of columns of data representing information about the objects. The information may include any of the data collected about an object, its metadata or its behaviour, sent to the base computer 3 by the remote computers 2. This may include any of the following for example: the name of the file, and the location (path) of the file, the country where the object was first encountered, the identity of the remote computer that encountered the object, its operating system and version number, details of the web browser and any other security products installed on the computer, the creator of the file, the icon associated with the file, etc. The information may include metadata about the file, such as the author or the size of the object or information relating to executable instructions in the object. The data may contain "actor" and "victim" information and details of its registry key. The information may include information about whether or not the object has been identified as safe or unsafe at the remote computer 2 or at the FX server 61.

The information displayed may contain counts of how often a particular attribute is present among all the objects returned by the query or across the community. In addition, the information may contain less easily understood information. As discussed above, the information collected about an object can include checksums of parts of the executable, e.g. the first 500 bytes of the executable part of the file. In many cases, the actual value of the checksum or other data is of little or no interest to the user. Therefore, preferably some or all of this information is presented to the user in a graphical way, utilising colour, shape and or different symbols, which makes spotting patterns in the data more intuitive and speedy for the user.

Preferably, at least one column of data is presented according to the following scheme:-

1) if the value is unique in that column between the rows of data representing objects then the numeral "1" is presented.

2) if the value is replicated between the rows of data on the screen, or between all the rows of data matching that query, then a coloured symbol (e.g. a green triangle or a

red letter "P" in a blue square, etc.) is allocated for that value and displayed in that column for all rows that share that value. Thus, without needing to know what the symbols represent, the user can see at a glance which rows on the screen have commonality of an attribute.

This provides a starting point for running further queries. For example, the user can quickly see commonality between objects which look interesting. As explained elsewhere in this document, a typical trait of malware is that the objects use a large number of file names, file locations, similar file sizes, similar code portions, etc. The program allows a user to refine a query by for example clicking on columns in the table and using the query creating tools 106 to add a particular attribute value to the predicate of the query, or to start a new query with this column value in the predicate, etc.

The ultimate aim of this process is for the user to find a query that returns the maximum number of rows with commonality. By this process, the user identifies a set of criteria made up of hashes and other metadata definitions that can be used to accurately identify similar objects that share criteria. For example, Figure 11 shows a user query that returns rows with a high degree of commonality representing objects that have commonality. The software also preferably allows the user to bring up a screen of statistics for the objects that have been returned from the query. In particular, as shown by Figure 12, the interface can display to the user the number of objects returned by the query that are known to the database as being malware, the number known as being not malware, and the number where it is not yet known whether or not the object is malware (represented in Figure 12 by differently shaded/coloured bars). Other data about the results of a query or objects having a certain attribute selected by the user can be shown in graphical form, e.g. a bar graph, or a pie diagram as shown in Figure 13. The user can take this information into account as well as information shown in the table 105 when deciding whether or not the results of the query determine malware. The user can then take the appropriate action, such as tagging the objects returned by the query as malware, not malware, or suspicious and requiring further investigation. Thus, by being able to query and analyse the collective view of an object, i.e. its metadata and behaviours, across all agents 10 that have seen it, a more informed view can be derived, whether by

human or computer, of the object. In addition it is possible to cross-group objects based on any of their criteria, i.e. metadata and behaviour.

To take an example, it might be a previously identified trait of certain types of malware that the malevolent object is located in the "recycle bin" of the operating system. This gives a starting point for the user to run a query to find all objects, or all objects encountered during a user specified time frame, that are located in the recycle bin by looking at their "path" attribute. This would display rows to the user corresponding to the different objects found (e.g. each row corresponding to a different MD5 signature). The user can then drill down through the rows by selecting interesting attributes by clicking on a value in a column. For example, the user may choose objects whose attributes show that the object's icon is the same as the icon used the "Notepad" program (which comes with Microsoft Windows (RTM) operating systems), but which are not Microsoft originating programs. The system preferably allows the user to apply Boolean operators in refining the query. The system allows the user to bring up statistics of how well the query cover objects that are known by the system to be malevolent or benign to give the user more information about useful the query is in classifying objects.

The users employed in grouping objects according to this scheme need not be highly skilled malware analysts. The users need only basic training in use of the tool and in grouping objects by running queries and looking for commonality. The final analysis of objects covered by the query can be taken by a skilled malware analyst. The advantage of this system is that the computer is doing the work in processing the raw data which is too large of a task to be practical for a human operator to complete. The human operators grouping the data need not be skilled, which reduces costs for the business. This reduces costs and leaves the skilled malware analysts to concentrate on queries that are found to be good candidates for further investigation. Thus, the skill of these operators is most effectively deployed in using their experience to identify malware.

Referring to Figure 9, if at stage 103 the user decides that a query (Q5) is deterministic in classifying the objects returned by a query as safe or unsafe, then the

rule can be passed back to the web servers 61 and or the agent program 10 at the remote computers 2 and used in real time in deciding whether new objects seen at the web servers 61 or remote computer 2 are safe or unsafe.

If a new object that has not been seen before by the community is received by a remote computer 2 or a web server 61 and is deemed by one of the rules run by the remote computer 2 or web server 61 to be unsafe, the object can be stopped from running on the remote computer 2 in real time, or the user of the remote computer 2 can be warned and given the option of continuing or not. Furthermore, the remote computer 2 (via the web server 61 to which it is assigned) or the web server 61 can report to the ENZO server 74 that a new object has been determined to be safe or unsafe by the rule. The ENZO server 74 can update its master database with this finding and this finding can be communicated to other remote computers 2 and or web servers 61 and used to update their databases that objects with that signature are unsafe and should be blocked in the future, or safe and should be allowed to run.

Alternatively, the rule can be used by human analyst at the ENZO layer to monitor suspicious objects. Objects covered by the rule can be displayed to a human analyst and the analyst can then decide for each object in turn whether it is malevolent or benign, and mark the object accordingly. These determinations for each object are sent back to the web servers 62 and or agent software 10 and used to decide whether or not the object is allowed to run when encountered at the remote computers in real time. This method does not react as quickly to new threats, compared with applying the rules in real time at the web servers 62 and or agent software 10. However, it may be preferred in cases where it is desired to keep the number of "false positives" low, and or where a rule is found to be good at identifying suspicious objects which need further investigation before a firm determination can be made that they are malware.

Furthermore, this action can be semi automated. The application can monitor the groupings along with any and all actions taken such as groups being determined as malicious or as benign. By tracking these actions it is possible for the ENZO server 74 to learn from human analysts how to identify and determine objects automatically. The

application can preferably remember queries that have been run by users. If the same query is being run repeatedly by a user and returning malware objects, or if a researcher consistently takes the action of determining the objects to be malware, then the system can automatically identify this condition and create a rule of the criteria and the action to determined matching objects as malicious. This rule can be sent to the FX server layer 60 to enable real time actions to be made to catch objects that match the rule and determine them as malicious. The identity of these rules and of malware grouping applied by the rules can then be fed back to both the agent and the ENZO server 74. In this way the FX server 61 is performing an action sanctioned and distributed by the ENZO server 74, on its behalf. Similarly, these same processes can be applied to benign groups of objects resulting in rules that determine such objects as "good" which can be propagated back to the FX layer 60 in the same way for the rules for "bad" objects. Thus, the ENZO layer 70 allows the user to easily identify these groupings. The ENZO layer can then monitor the groupings along with any and all actions taken such as groups being determined as malicious or as benign. By tracking these actions it is possible for the ENZO layer 70 to learn from humans how to identify and determine objects automatically.

The ENZO layer 70 can also monitor trends and bring information to the human analysts' attention, such as the evolution in the behaviour of a previously known good program. For example, a legitimate version of the game Solitaire will be observed by the ENZO servers 74 to have a particular behaviour profile from the actions performed by that program on remote computers over a period of time. If after a period of time that program starts exhibiting new, suspicious behaviour, such as trying to install a driver or accessing a web server in another country, this can be flagged for investigation.

Furthermore, preferably the agent program 10 at the remote computer provides an interface that allows the user to report “false positives” to the system, i.e. where an object has been flagged as malware which the user believes to be legitimate software. The system is arranged to feedback this information to the ENZO server 74. At this point, the system can determine that the rule is no longer reliably deterministic in finding malware and can disable the rule. Alternatively the system can flag the rule for manual

review and or modification by a human analyst. Alternatively, it can be decided that the rule is generally useful despite the false positive and that the false positive is an outlier. The conflicting benign object can then be specifically excluded from the rule at the FX layer 70 by placing it on a white list.

It should be noted that rules can be prioritised (applied in order by priority) and can be established to only apply against objects having a specific determination, location, popularity, age or any other criteria known by or derived by the database. For example, if a first rule determines the object originates from Microsoft, then it may be decided not to apply any further rules. In contrast, if a first rule determines that an object is suspicious, then it may be decided to apply further rules as appropriate.

Thus, the preferred software application running on an ENZO server 74 provides powerful object behaviour monitoring and assessment. The software allows the user to obtain a thorough understanding of an object's behaviour on a remote computer and the contextual environment in which it is observed, in part through providing powerful data visualisation techniques. The software enables large research teams to work collaboratively and incrementally and leverages human research skills and experience through expert system automation.

CONFIGURABLE FIREWALL

It is desirable to stop malware before a computer becomes infected, e.g. when the infected file is received by email, downloaded, or when it is installed or run for the first time.

A well known example of a malware program is the “Zeus” Trojan. This program runs in the background on an infected computer and steals login details as they are entered on screen by a user by monitoring the user’s keystrokes. This information is then sent to the criminal’s servers where it can be used to take control of the infected computer. An instant message is sent to the criminal over the network when the malware

program detects logon information being entered on an online banking website, so the criminal receives this information in near real time. The Trojan can then take remote control of the user's computer using the Virtual Network Connection protocol, a protocol that allows a remote user to access and take control of a computer remotely. The criminal can then steal money from the victim's bank account.

While most anti-malware software attempts to stop the malware from infecting a host computer or stopping communications with the malware as soon as possible, not much attention has been shown to finding and prosecuting the criminals responsible. One difficulty is that it is illegal for the anti-malware or even the police to hack into the criminal's servers to find the criminal's data. Indeed, it a known ruse for the criminals to use so-called "botnets", which are "zombie networks" of legitimate users' computers which have been infected by malware and are thereby under the control of the criminals.

The preferred embodiment as illustrated by Figure 14 implements a firewall 95 with the agent program 10 at the remote computer 2. A firewall per se is well known. However, normally firewalls are configured by rules input by the user to govern what programs have permission to access the network for incoming/outgoing traffic. The preferred embodiment additionally takes rules from the base computer 3 to limit which objects on the remote computer 2 can communicate across the firewall and with which entities 96,97 on the network. For example, information can be sent from the base computer 3 to the firewall 95 that known active URLs of Zeus servers 97 are blocked from exchanging messages from all objects on the remote computer 2. Thus, the firewall 95 can implement a rule blocking communications with the criminal's servers.

This provides a valuable second line of defence against malware. It is generally desirable to stop malware at the point of infection by preventing the malware from infecting a computer. The next line of defence is to stop the malware communicating. The configurable firewall 95 can therefore leverage the rules and knowledge developed about malevolent objects and network URLs held at the base computer 3 to provide a next line of defence in fighting malware.

Furthermore, in a preferred embodiment, the agent program 10 can be used to contact the authorities 98, e.g. a law enforcement agency, if malevolent internet traffic is detected. The IP traffic between the infected computer 2 and the criminal's server 97 can be intercepted by the firewall 95, stored and sent to the authorities' server 98, so the authorities can see what information the criminals were stealing through the malware. This information can be sent to the authorities' servers 98 in encrypted form for added security. In the preferred embodiment, checksums are made and stored of the data that sent to the authorities' servers 98, as there are very strict processes in place for forensic data handling and evidence retention that should be observed.

Legal constraints will mean in most instances it is necessary to obtain permission from the user of the infected computer 2 before this information is captured and sent to a third party. In this situation, the agent program 10 will open a dialogue with the user to obtain permission before proceeding. In some instances, the user may be happy to give blanket permission for data to be sent whenever a malware program or a particular class of malware program is detected on his computer 2, so it will not be necessary to obtain specific permission every time malevolent objects or communication is detected.

SELF DEFENCE

Malware has evolved to the state where it will attack, disable or otherwise destroy security products installed on a computer.

There are two principle vectors which need to be considered.

A first approach is to target the methods used by malware to identify security products. In this specific case the malware will use behaviour monitoring of processes running on the remote computer that view, observe, record, examine or otherwise interfere any aspect of the malware code. Examples might be a malware entity watching for processes or tasks which look at the registry keys the malware has used to configure, control or record its operation. As will be appreciated, malware is by its nature

surreptitious. From the malware's point of view, no processes on the remote computer should be monitoring or interacting with the malware object, since the existence of the malware object on the local computer should be unknown. If any processes are monitoring the malware, it is therefore likely to be security software or a system monitoring tool or a system tool being used by the user of the computer 2 to rid the computer 2 of the infection.

Thus, by finding processes that are doing this, the malware process can find the identity of the process and its location or locations on disk. This identification then allows it the ability to delete, disable or interfere with the process or processes it has identified as potential threats. In most cases these will indeed be security programs or system monitoring tools, both which it might consider threats.

A preferred embodiment of the present invention guards against this possible interference by malware programs by preventing the behavioural detection of a security program when examining the malware. This is achieved by hiding behind, masquerading as and or leveraging core operating system components to examine the malware's state and components. In particular, the agent program 10 performs operations by impersonating the system's context when it is necessary to rely on standard system calls, or circumventing any system calls by accessing data at the raw level as it is stored on disk. For example, the agent program 10 can directly impersonate the kernel of the operating system when calling the ZwTerminateProcess function to terminates a malevolent process. In doing so, the malware cannot trace the call back to the agent program. The malware considers this behaviour as normal, as it expects the operating system to interact with it (e.g. it is necessary for the operating system to be able to terminate the process when the computer is shut down), and so the malware does not attempt to terminate the agent program process. Furthermore, the malware cannot react by killing the process as the process is only identifiable as the operating system itself. To kill the operating system would also prevent the malware from operating.

Figure 15 shows a hierarchy of control on a computer system 2 going from the kernel level 92 at the lowest level, the operating system level 91, and a web browser

running 92 on the operating system 91. A second consideration is that, for malware to assert maximum control over the operation of the computer, it will often attempt to install a driver, possibly a kernel mode driver, which has complete control over processes and actions performed. A type of malware commonly known as a "rootkit" operates in this way and can, among other things, be used to conceal other malware, notably password-stealing key loggers and computer viruses. In certain cases the malware will load a malicious driver and use this to disable security applications and drivers from starting when Windows starts. In particular, the malware may have a list of drivers or program components that it knows correspond to security products.

To prevent malware from using this approach to disabling security applications the agent program 10 dynamically creates a second or backup driver or component 94 which loads as a backup of main component 93 during installation or bootup in the event that the main components 93 are inaccessible (as shown by Figure 14). It would have identical functionality but would be modified so as to appear different by name and form. This can be randomised, so that the malware cannot learn to identify the security program. In this scenario should the primary component fail to load, most likely due to being killed by malware, the second driver 94 would be loaded to perform its function. If the primary component 93 loads successfully, the secondary component 94 would simply terminate to avoid conflict by identifying the presence of the primary component 93. By randomising the filenames and checksums of the installed objects comprising the agent program 10, the agent program 10 is able to evade heuristic detection by active threats that would attempt to terminate or remove critical agent components.

Later versions of Microsoft's Windows operating system provide enhanced security by requiring system and low level drivers to be signed. This policy, called the kernel mode code signing policy, disallows any unauthorized or malicious driver to be loaded. Some malware creations modify the master boot record to nullify driver certification checks. The malware executed by an infected master boot record bypasses driver signing policy by changing the boot options of Microsoft boot programs that will allow an unsigned driver to load.

So, in these conditions the secondary driver or component could remove its own digital signature to evade detection by the malware. This means it would fail to load unless the master boot record had been modified to disable driver verification. So it represents no threat to an uninfected system and would never load unless the system was infected and the master boot record was modified.

Embodiments of the present invention have been described with particular reference to the examples illustrated. However, it will be appreciated that variations and modifications may be made to the examples described within the scope of the present invention.

CLAIMS

1. A method of classifying a computer object as malware, the method comprising:

at a base computer, receiving data about a computer object from each of plural remote computers on which the object or similar objects are stored and or processed;

wherein the base computer comprises plural threat servers arranged to receive said data from the plural remote computers and apply rules and or heuristics against that data in real time to determine whether or not said object is malware and to communicate said determination to the remote computers;

said base computer further comprising at least one central server in communication with the threat servers and arranged to receive said data about objects from the threat servers to maintain a master database of data received about objects from all of the threat servers.

2. A method according to claim 1, wherein at least one threat server comprises at least one database for holding information received from remote computers to which it is attached, the method comprising:

storing said data in at least one database at the threat server; and,

at intervals, storing the contents of the database in storage together with a timestamp and clearing the database.

3. A method according to claim 2, comprising creating a backup central server by receiving at a central server all of the timestamped blocks of data and incorporating them into its database.

4. A method according to claim 2 or claim 3, comprising:

taking a central server off-line for a period of time such that it does not receive updates of data from the threat servers during that period of time;

after the period of time has elapsed, updating the database of the central server with timestamped blocks of data from the storage that have a timestamp later than the time when the central server went off-line; and,

bringing the central server back on line.

5. A method according to claim 2 or claim 3, comprising rolling back the database of a central server to a point of time in the past; and,

updating the database of the central server with timestamped blocks of data from storage that have a timestamp later than said past point of time; and,

bringing the central server back on line.

6. A method according to any of claims 2 to 5, wherein the central server has databases including any one or more of:

a) object signatures and metadata about that object;

b) object behaviour; and,

c) information about what objects are present on what remote computers.

7. A method according to any of claims 1 to 6, wherein said threat and central servers are implemented using cloud computing.

8. A method according to any of claims 1 to 7, comprising:

maintaining at a threat server, a list of objects previously seen at that threat server and forwarded to the central server; and,

if an object has not been seen before, sending the data about that object to the central server,

and if an object has been seen before, increasing the count for that object instead of sending the data.

9. Apparatus for classifying a computer object as malware, the apparatus comprising:

a base computer arranged to receive data about a computer object from each of plural remote computers on which the object or similar objects are stored and or processed;

wherein the base computer comprises plural threat servers arranged to receive said data from the plural remote computers and apply rules and or heuristics against that

data in real time to determine whether or not said object is malware and to communicate said determination to the remote computers;

said base computer further comprising at least one central server in communication with the threat servers and arranged to receive said data about objects from the servers to maintain a master database of data received about objects from all of the threat servers.

10. Apparatus according to claim 9, comprising at least one database, the threat servers being arranged to store said data information received from remote computer in the database;

the apparatus comprising storage, the threat servers being arranged to, at intervals, store the contents of the database in storage together with a timestamp and clearing the database.

11. Apparatus according to claim 10, comprising a backup central server having a database, the database of the backup central server being populated by receiving at the backup central server all of the timestamped blocks of data from the storage and incorporating them into the database.

12. Apparatus according to claim 10 or claim 11, wherein, in the event that a central server is taken off-line for a period of time such that it does not receive updates of data from the threat servers during that period of time, the central server is arranged to, after the period of time has elapsed, update its database with timestamped blocks of data from the storage that have a timestamp later than the time when the central server went off-line.

13. Apparatus according to claim 10 or claim 11, wherein, in the event that the database of a central server is rolled back to a point of time in the past, the central server is arranged to update its database with timestamped blocks of data from storage that have a timestamp later than said past point of time.

14. Apparatus according to any of claims 9 to 13, wherein the central server has databases including any one or more of:

a) object signatures and metadata about that object;

b) object behaviour; and,

c) information about what objects are present on what remote computers.

15. Apparatus according to any of claims 9 to 14, wherein the threat and central servers are implemented using cloud computing.

16. Apparatus according to any of claims 9 to 14, wherein a threat server is arranged to maintain a list of objects previously seen at that threat server and forwarded to the central server; and,

if an object has not been seen before, the threat server is arranged to send the data about that object to the central server,

and if an object has been seen before, the threat server is arranged to increase the count for that object instead of sending the data.

17. A method of classifying a computer object as malware, the method comprising:

at a base computer, receiving data about a computer object from each of plural remote computers on which the object or similar objects are stored and or processed;

counting the number of times in a given time period objects having one or more common attributes or behaviours that have been seen by the remote computers;

comparing the counted number with the expected number based on past observations; and,

if the comparison exceeds some predetermined threshold, flagging the objects as unsafe or as suspicious.

18. A method according to claim 17, wherein the attribute of the object is one or any combination of: the file name, the file type, the file location, vendor information contained in the file, the file size, registry keys relating to that file, or any other system derived data, or event data relating to the object.

19. Apparatus for classifying a computer object as malware, the apparatus comprising a base computer arranged to receive data about a computer object from each of plural remote computers on which the object or similar objects are stored and or processed; the base computer being arranged to:

count the number of times in a given time period objects having one or more common attributes or behaviours that have been seen by the remote computers;

compare the counted number with the expected number based on past observations; and,

if the comparison exceeds some predetermined threshold, flag the objects as unsafe or as suspicious.

20. Apparatus according to claim 19, wherein the attribute of the object is one or any combination of: the file name, the file type, the file location, vendor information contained in the file, the file size, registry keys relating to that file, or any other system derived data, or event data relating to the object.

21. A method of classifying a computer object as malware, the method comprising:

at a base computer, receiving data about a computer object from each of plural remote computers on which the object or similar objects are stored and or processed;

storing said data in a database; and,

presenting the user with a display of information relating to a group of plural objects and various attributes of those objects, the display being arranged such that commonality is shown between objects, wherein the group of objects displayed correspond to a user query of the database.

22. A method according to claim 21, wherein the information is displayed in tabular form with rows of the table corresponding to objects and columns of the table corresponding to attributes of the objects.

23. A method according to claim 21 or claim 22, wherein at least one attribute of the objects is presented to the user pictorially such that objects with common attributes are given the same pictorial representation.

24. A method according to claim 23, wherein the pictorial representation comprises symbols having different shapes and/or colours.

25. A method according to any of claims 21 to 24, comprising:
identifying commonality in one or more attributes between objects; and,
refining the query in accordance with said identified commonality.

26. A method according to any of claims 21 to 25, comprising creating a rule from a user query if it is determined that the query is deterministic in identifying malware.

27. A method according to any of claims 21 to 26, comprising:
monitoring user groupings of objects along with any and all user actions taken such as classifying the objects of the group as being safe or unsafe; and,
automatically applying said groupings and actions in generating new rules for classifying objects as malware.

28. A method according to claim 26 or claim 27, comprising applying the rule to an object at the base computer and or sending the rule to a remote computer and applying the rule to an object at the remote computer to classify the object as safe or unsafe.

29. A method according to claim 28, comprising storing the classification of an object as safe or unsafe according to the rule in the database at the base computer.

30. A method according to any of claims 26 to 29, comprising:
receiving information from a remote computer that an object classified as malware by said rule is believed not to be malware; and,
amending or deleting the rule in accordance with said information.

31. Apparatus for classifying a computer object as malware, comprising a base computer arranged to receive data about a computer object from each of plural remote

computers on which the object or similar objects are stored and or processed; the base computer being arranged to:

store said data in a database; and,

present the user with a display of information relating to a group of plural objects and various attributes of those objects, the display being arranged such that commonality is shown between objects, wherein the group of objects displayed correspond to a user query of the database.

32. Apparatus according to claim 31, wherein the base computer is arranged to display the information in tabular form with rows of the table corresponding to objects and columns of the table corresponding to attributes of the objects.

33. Apparatus according to claim 31 or claim 32, wherein at least one attribute of the objects is displayed pictorially such that objects with common attributes are given the same pictorial representation.

34. Apparatus according to claim 33, wherein the pictorial representation comprises symbols having different shapes and/or colours.

35. Apparatus according to any of claims 31 to 34, wherein the base computer is arranged to:

identify commonality in one or more attributes between objects; and,

refine the query in accordance with said identified commonality.

36. Apparatus according to any of claims 31 to 35, wherein the base computer is arranged to allow the user to create a rule from a user query if it is determined that the query is deterministic in identifying malware.

37. Apparatus according to any of claims 31 to 36, wherein the base computer is arranged to monitor user groupings of objects along with any and all user actions taken such as classifying the objects of the group as being safe or unsafe; and to automatically

apply said groupings and actions in generating new rules for classifying objects as malware.

38. Apparatus according to claim 36 or claim 37, wherein the base computer is arranged to apply the rule to an object at the base computer to classify the object as safe or unsafe, and or arranged to send the rule to a remote computer such that the remote computer can apply the rule to an object at the remote computer.

39. A method according to claim 38, wherein the base computer is arranged to store the classification of an object as safe or unsafe according to the rule in the database at the base computer.

40. Apparatus according to any of claims 36 to 39, wherein the base computer is arranged to receive information from a remote computer that an object classified as malware by said rule is believed not to be malware; and to amend or delete the rule in accordance with said information.

41. A method of operating a security program on a computer, comprising operating the security program to impersonate or use operating system functions in monitoring objects running on the computer, said monitoring being to determine whether the objects are malware.

42. A computer program for fighting malware, the computer program comprising program instructions which when run on a computer program cause the computer to monitor objects running on the computer to determine whether the objects are malware or not, the monitoring being such that the program impersonates or uses operating system functions.

43. A method of operating a security program on a computer, comprising:

loading a first component of the security program on the computer;

dynamically creating a second component of the security program on the computer having different attributes from the first component and which will

automatically load in the event that the first component fails to load due to malevolent activity.

44. A method according to claim 43, wherein the second component is arranged to remove its own digital signature.

45. A computer program for fighting malware, the computer program comprising program instructions which when run on a computer program cause the computer to load a first component of the security program on the computer; and to dynamically create a second component of the security program on the computer having different attributes from the first component and which will automatically load in the event that the first component fails to load due to malevolent activity.

46. A computer program according to claim 45, wherein the second component is arranged to remove its own digital signature.

47. A computer program according to claim 42, 45 or 46 recorded on a carrier.

48. A method of connecting a remote computer to one of a plurality of servers, the method comprising:

installing an agent program on the remote computer; the agent program having an algorithm for allocating the remote computer to a server determined by the time when the agent program was installed; and,

connecting the agent program to the allocated server.

49. A method according to claim 48, wherein the algorithm allocates the remote computer to a server determined also by the proximity of the remote computer to the servers.

50. A method according to claim 48 or claim 49, comprising connecting the remote computer to a different server in accordance with information received by the agent program from the originally allocated server.

51. A method according to any of claims 48 to 50, wherein the agent program has a secondary algorithm to determine a secondary server for the remote computer in case the originally allocated server is inaccessible.

52. A computer program comprising program instructions for:

allocating the remote computer to one of a plurality of servers determined by the time when the program was installed on the remote computer; and,

connecting the agent program to the allocated server.

53. A computer program according to claim 52, wherein the computer program allocates the remote computer to a server determined also by the proximity of the remote computer to the servers.

54. A computer program according to claim 52 or claim 53, wherein the computer program is arranged to connect the remote computer to a different server in accordance with information received by the agent program from the originally allocated server.

55. A computer program according to any of claims 52 to 54, wherein the program determines a secondary server for the remote computer to connect to in case the originally assigned is inaccessible.

56. A computer program according to any of claims 52 to 55 recorded on a carrier.

57. A method of providing protection against malware, the method comprising:

executing an agent program on a remote computer connected to a network, the agent program being configured to communicate with a base computer via the network, the agent program including a firewall arranged to block communications between the remote computer and entities on the network in accordance with predetermined rules; and,

configuring the firewall in accordance with rules received from the base computer.

58. A method according to claim 57, comprising:

receiving at the remote computer from the base computer information that an object on the remote computer and or an entity on the network is unsafe; and,

including a rule at the remote computer so that intended network communications involving the unsafe object and or unsafe entity are blocked by the firewall.

59. A method according to claim 57 or claim 58, comprising:

receiving at the remote computer from the base computer information that an object on the remote computer and or an entity on the network is unsafe;

asking permission from the user of the remote computer for details of intended network communications involving the unsafe object and or unsafe entity to be shared with a third party; and,

intercepting intended network communications involving the unsafe object and or the unsafe entity and sharing them with a third party.

60. A computer program for providing protection against malware comprising program instructions which when executed on a remote computer connected to a network:

communicate with a base computer via the network, the computer program including a firewall arranged to block communications between the remote computer and entities on the network in accordance with predetermined rules; and,

configuring the firewall in accordance with rules received from the base computer.

61. A computer program according to claim 60, comprising:

receiving at the remote computer from the base computer information that an object on the remote computer and or an entity on the network is unsafe; and,

including a rule at the remote computer so that intended network communications involving the unsafe object and or unsafe entity are blocked by the firewall.

62. A computer program according to claim 60 or claim 61, comprising:

receiving at the remote computer from the base computer information that an object on the remote computer and or an entity on the network is unsafe;

asking permission from the user of the remote computer for details of intended network communications involving the unsafe object and or unsafe entity to be shared with a third party; and,

intercepting intended network communications involving the unsafe object and or the unsafe entity and sharing them with a third party.

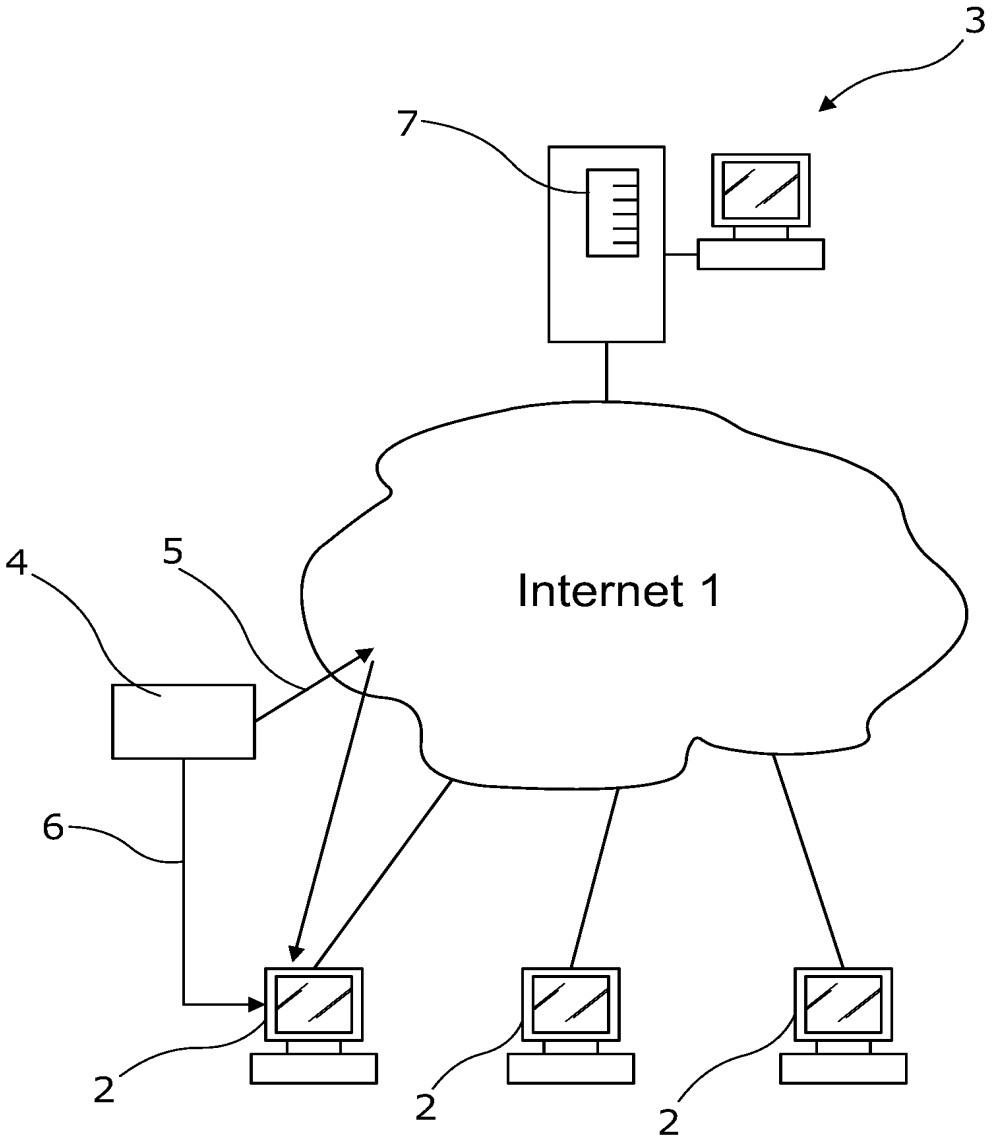


Fig. 1
(Prior Art)

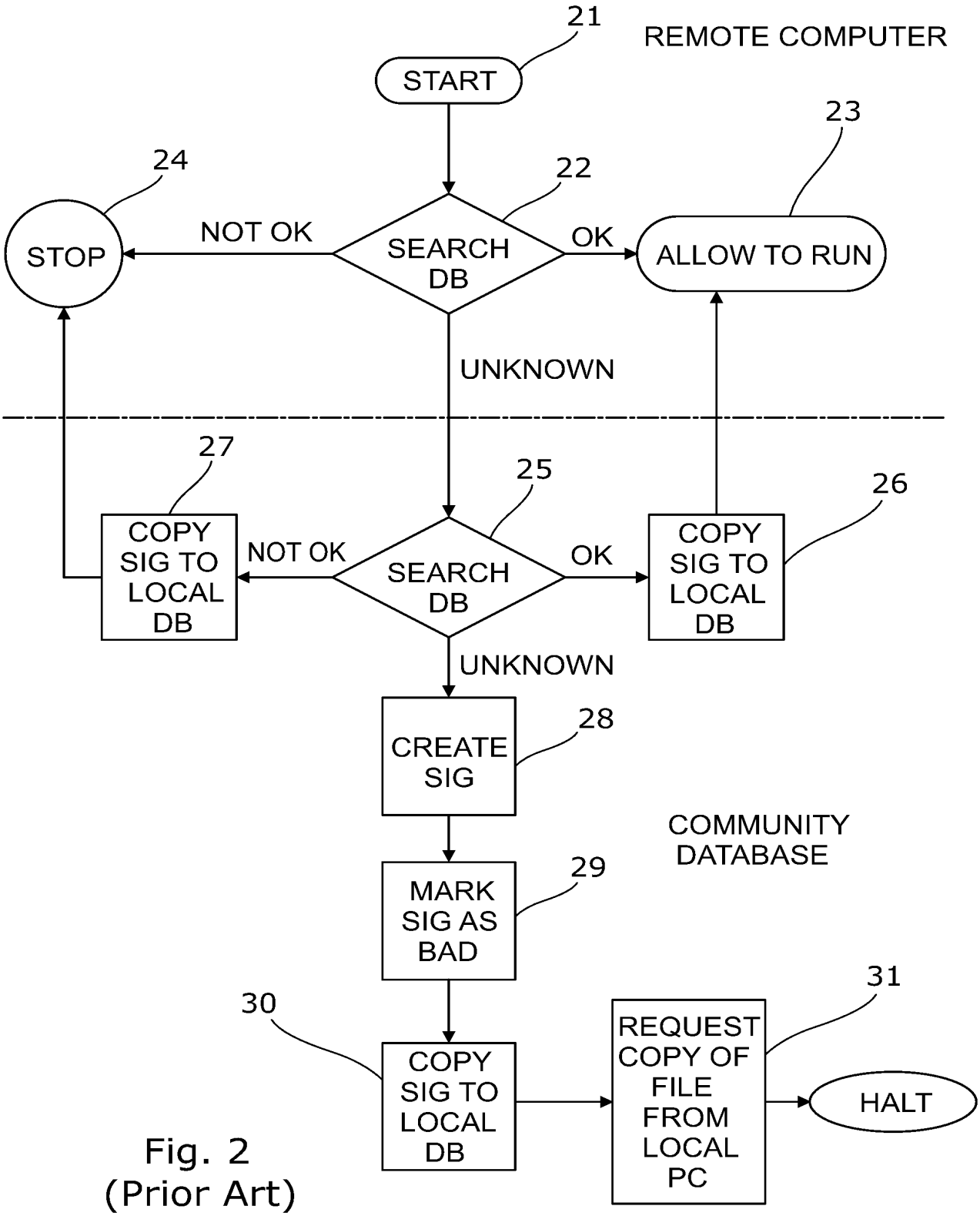


Fig. 2
(Prior Art)

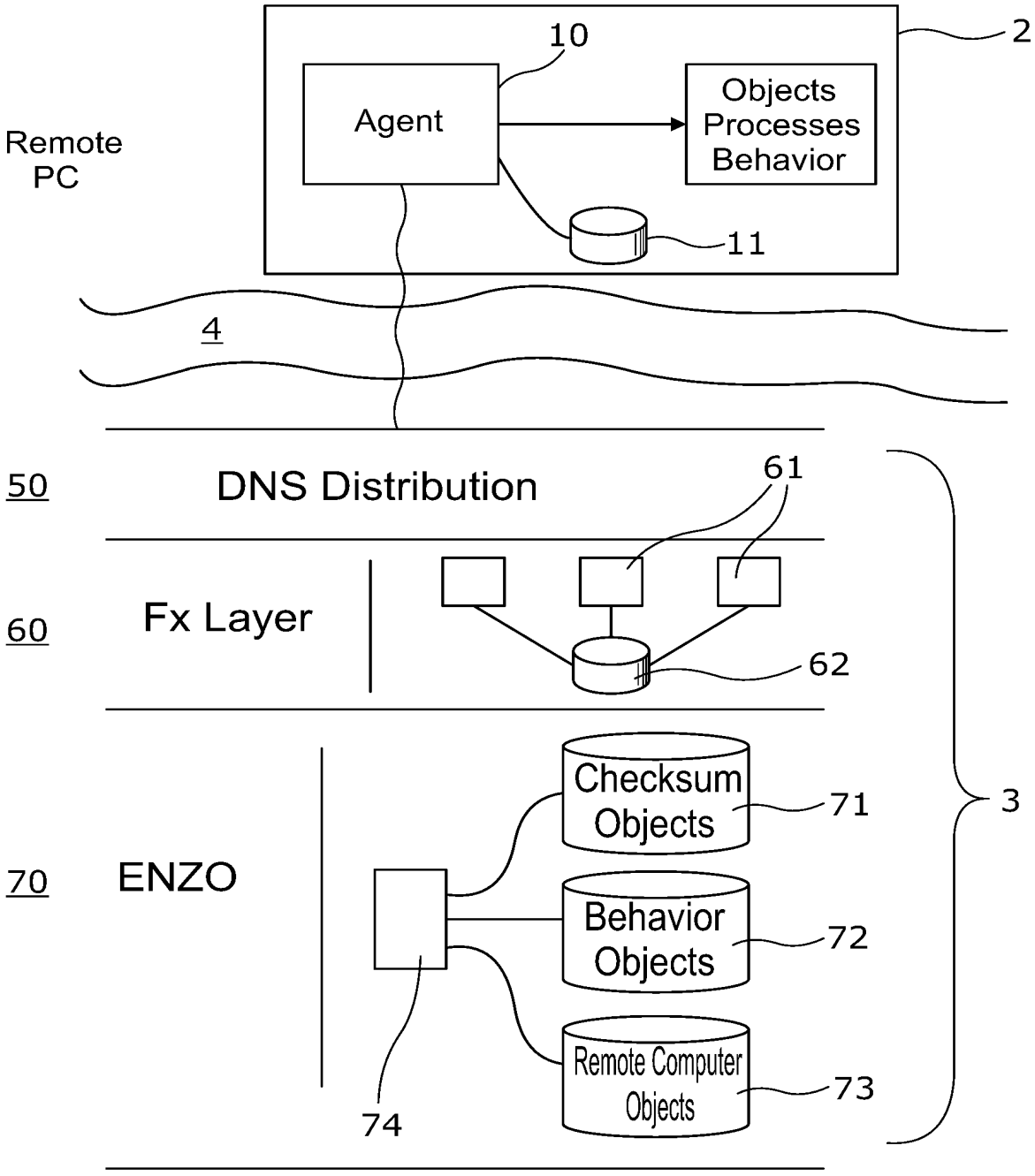

Remote PC
10
Agent
Objects Processes Behavior
2
11
4
50
DNS Distribution
61
60
Fx Layer
62
70
ENZO
Checksum Objects
71
Behavior Objects
72
Remote Computer Objects
73
74
3

Fig. 3

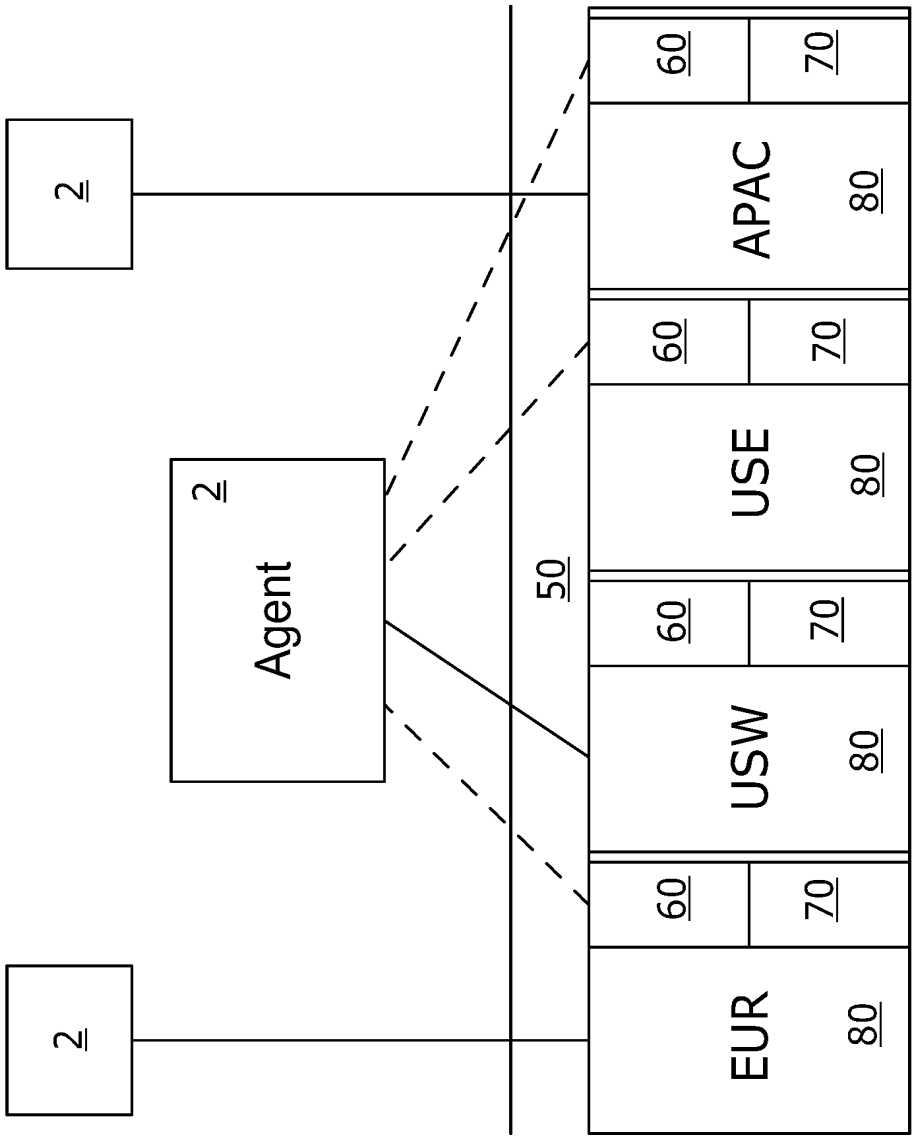


Fig. 4

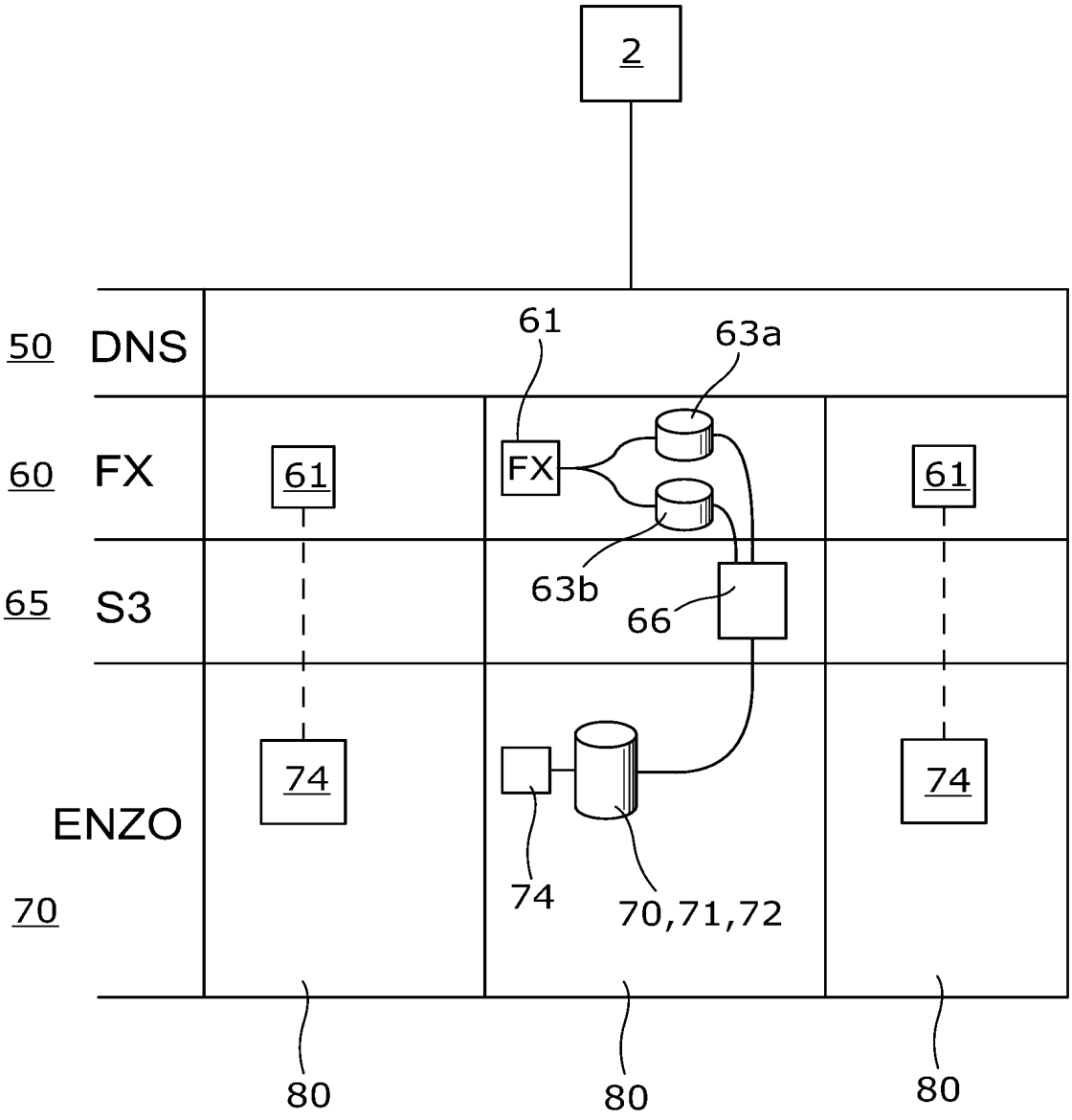

2
50 DNS
61
63a
60 FX
61
FX
61
63b
65 S3
66
74
74
ENZO
70
74
70,71,72
80
80
80

Fig. 5

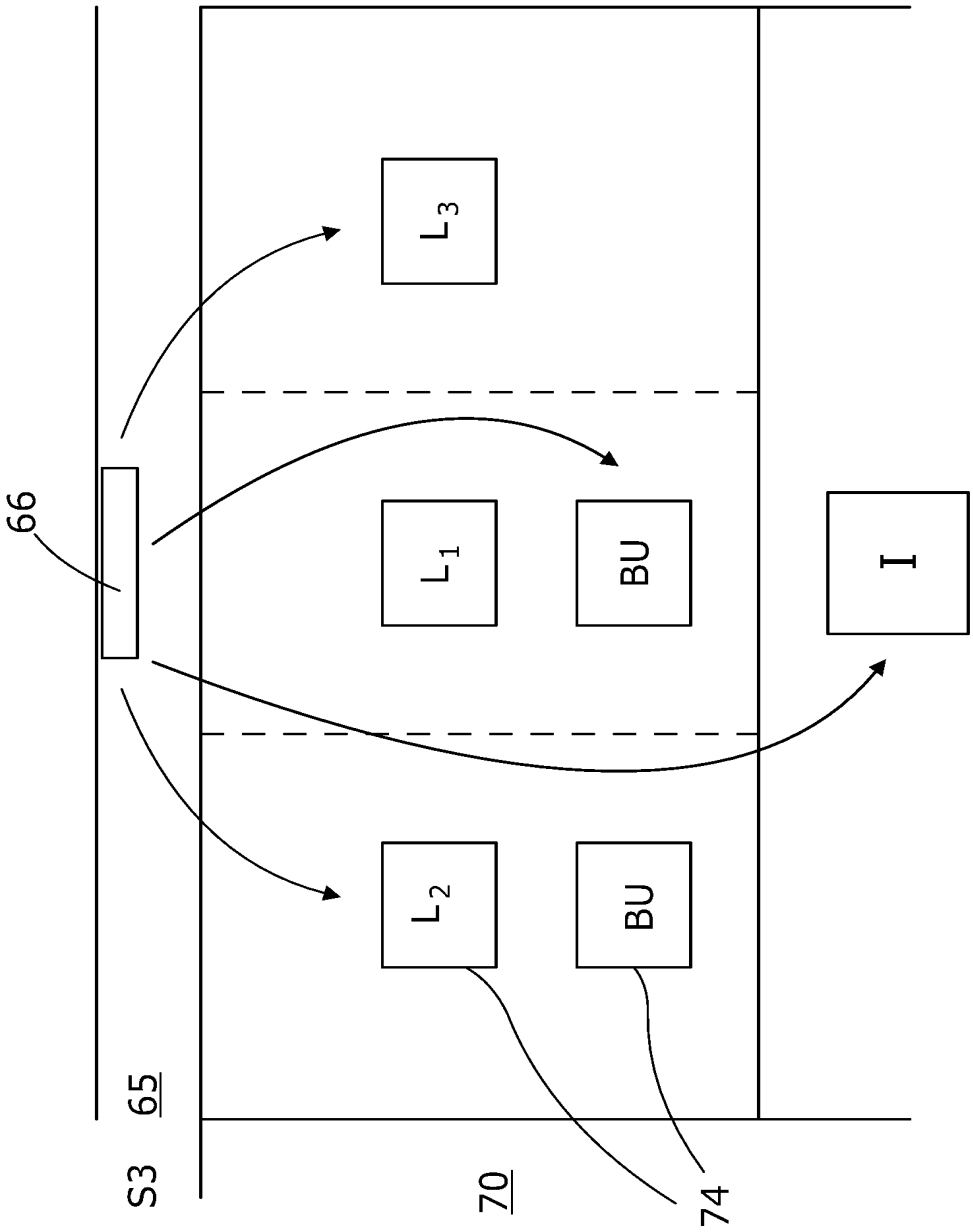


Fig. 6

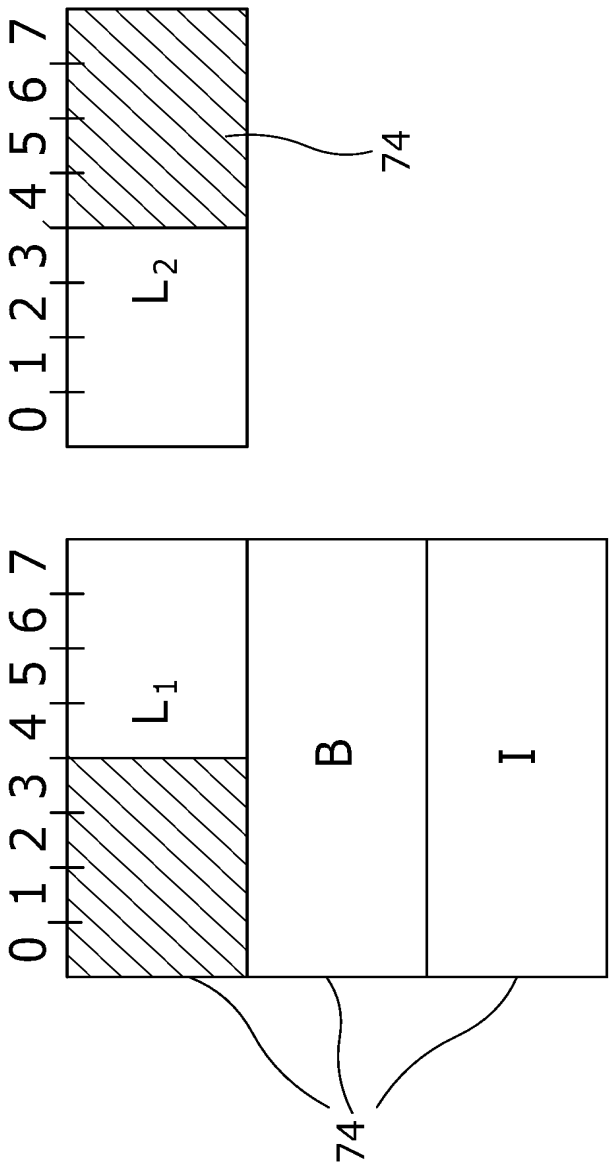


Fig. 7

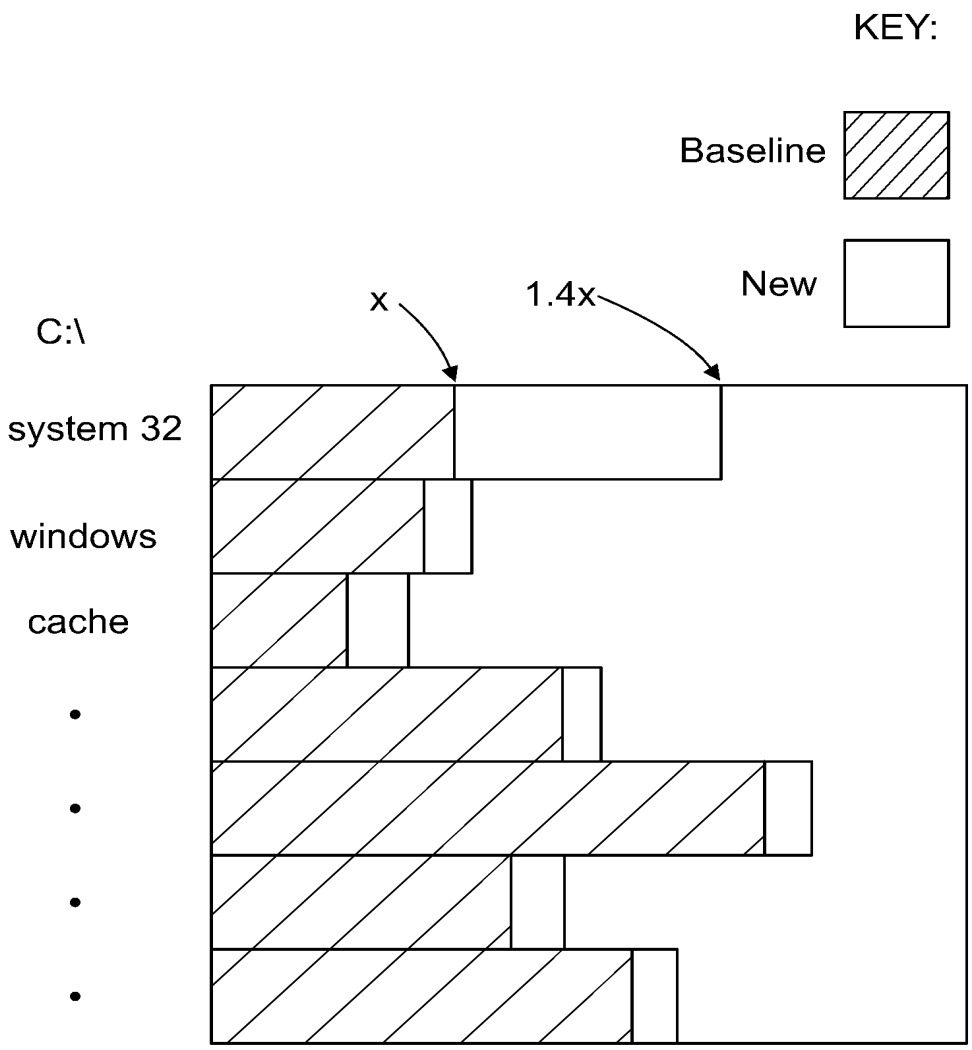


Fig. 8

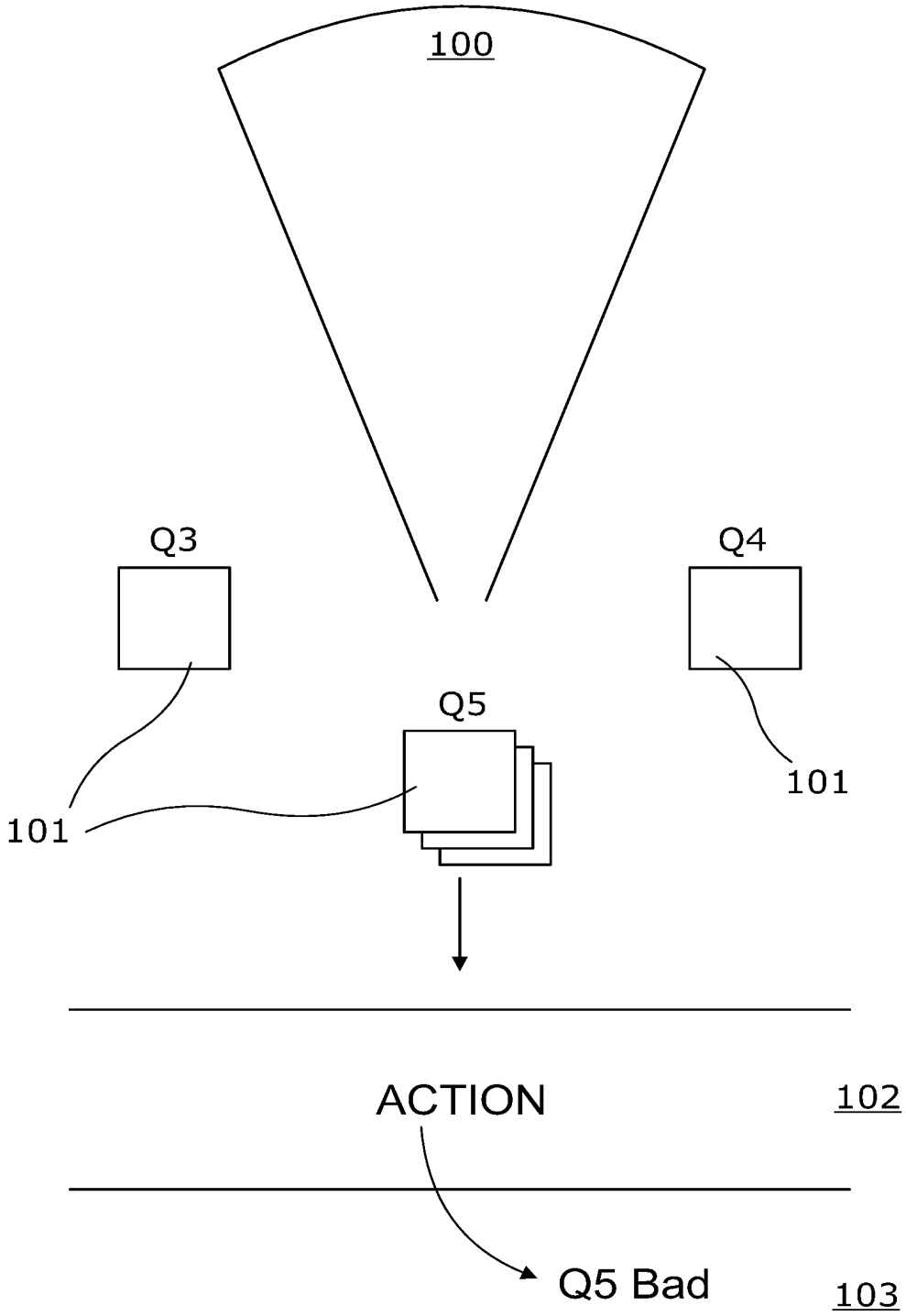
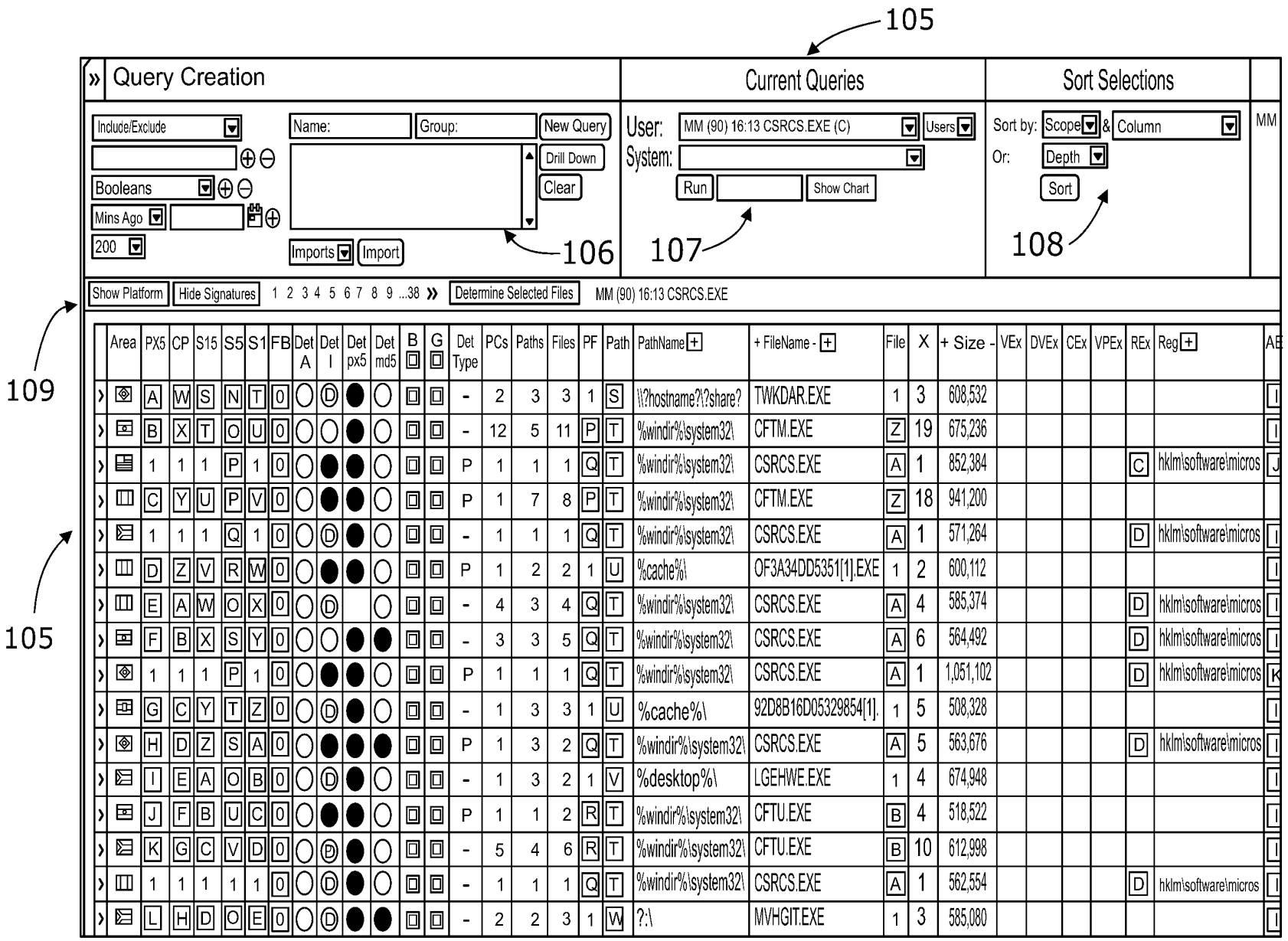


Fig. 9



	Area	PX5	CP	S15	S5	S1	FB	Det A	Det I	Det px5	Det md5	B	G	Det Type	PCs	Paths	Files	PF	Path	PathName	+ FileName -	File	X	+ Size -	VEx	DVEx	CEx	VPEx	REx	Reg	AB
›		A	W	S	N	T	0	○	Ⓓ	●	○	□	□	-	2	3	3	1	S	\\?hostname?\?share?	TWKDAR.EXE	1	3	608,532							
›		B	X	T	O	U	0	○	○	●	○	□	□	-	12	5	11	P	T	%windir%\system32\	CFTM.EXE	Z	19	675,236							
›		1	1	1	P	1	0	○	●	●	○	□	□	P	1	1	1	Q	T	%windir%\system32\	CSRCS.EXE	A	1	852,384					C	hklm\software\micros	J
›		C	Y	U	P	V	0	○	●	●	○	□	□	P	1	7	8	P	T	%windir%\system32\	CFTM.EXE	Z	18	941,200							
›		1	1	1	Q	1	0	○	Ⓓ	●	○	□	□	-	1	1	1	Q	T	%windir%\system32\	CSRCS.EXE	A	1	571,264					D	hklm\software\micros	
›		D	Z	V	R	W	0	○	●	●	○	□	□	P	1	2	2	1	U	%cache%\	OF3A34DD5351[1].EXE	1	2	600,112							
›		E	A	W	O	X	0	○	Ⓓ		○	□	□	-	4	3	4	Q	T	%windir%\system32\	CSRCS.EXE	A	4	585,374					D	hklm\software\micros	
›		F	B	X	S	Y	0	○	○	●	●	□	□	-	3	3	5	Q	T	%windir%\system32\	CSRCS.EXE	A	6	564,492					D	hklm\software\micros	
›		1	1	1	P	1	0	○	●	●	○	□	□	P	1	1	1	Q	T	%windir%\system32\	CSRCS.EXE	A	1	1,051,102					D	hklm\software\micros	K
›		G	C	Y	T	Z	0	○	Ⓓ	●	○	□	□	-	1	3	3	1	U	%cache%\	92D8B16D05329854[1].	1	5	508,328							
›		H	D	Z	S	A	0	○	●	●	●	□	□	P	1	3	2	Q	T	%windir%\system32\	CSRCS.EXE	A	5	563,676					D	hklm\software\micros	
›		I	E	A	O	B	0	○	Ⓓ	●	○	□	□	-	1	3	2	1	V	%desktop%\	LGEHWE.EXE	1	4	674,948							
›		J	F	B	U	C	0	○	●	●	○	□	□	P	1	1	2	R	T	%windir%\system32\	CFTU.EXE	B	4	518,522							
›		K	G	C	V	D	0	○	Ⓓ	●	○	□	□	-	5	4	6	R	T	%windir%\system32\	CFTU.EXE	B	10	612,998							
›		1	1	1	1	1	0	○	Ⓓ	●	○	□	□	-	1	1	1	Q	T	%windir%\system32\	CSRCS.EXE	A	1	562,554					D	hklm\software\micros	
›		L	H	D	O	E	0	○	Ⓓ	●	●	□	□	-	2	2	3	1	W	?:\	MVHGIT.EXE	1	3	585,080							

Fig. 10

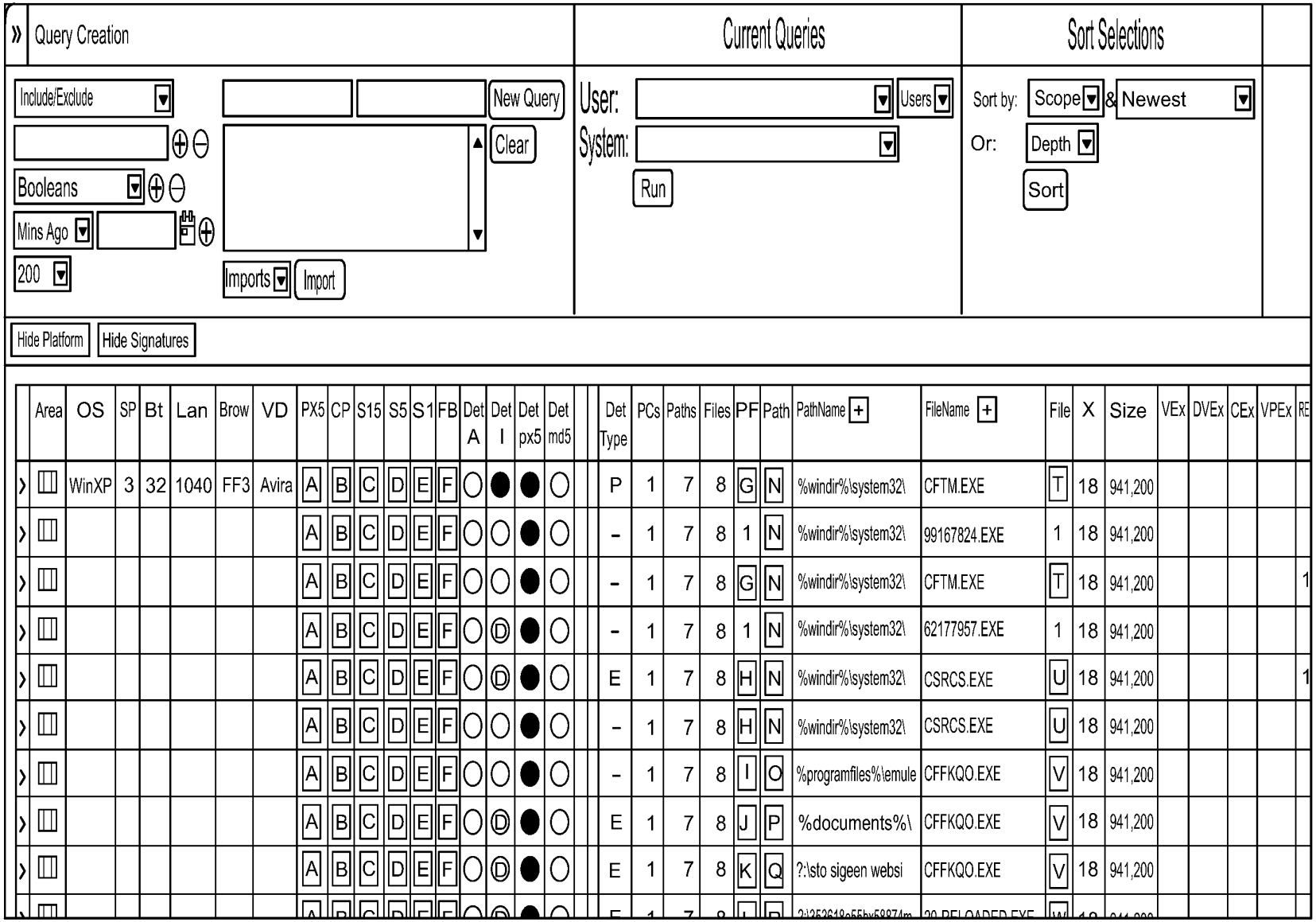
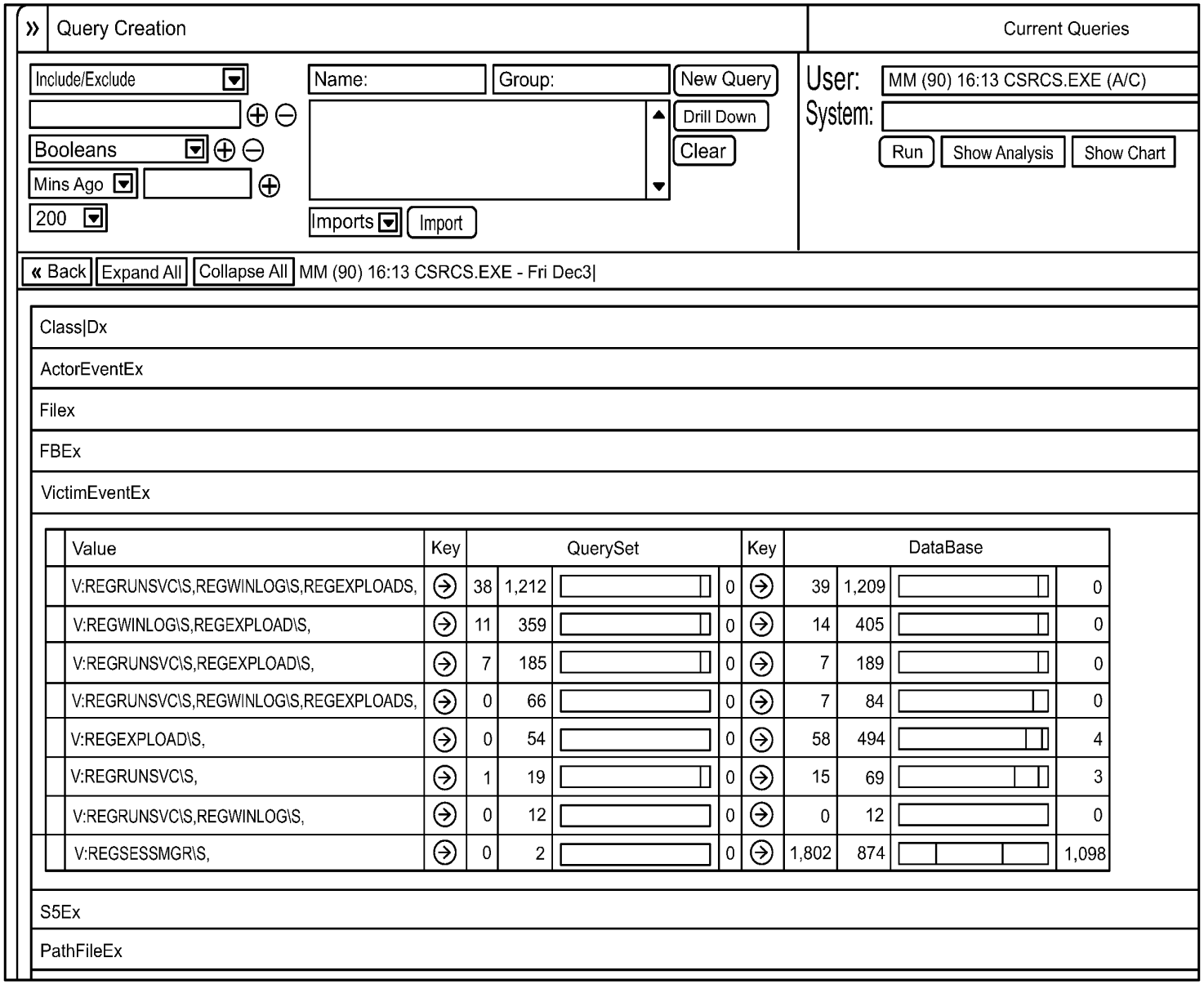

Query Creation
Current Queries
Sort Selections
Include/Exclude
New Query
Clear
Booleans
Mins Ago
200
Imports
Import
User:
Users
System:
Run
Sort by:
Scope
&
Newest
Or:
Depth
Sort
Hide Platform
Hide Signatures
Area OS SP Bt Lan Brow VD PX5 CP S15 S5 S1 FB Det A Det I Det px5 Det md5 Det Type PCs Paths Files PF Path PathName FileName File X Size VEx DVEx CEx VPEx RE
WinXP 3 32 1040 FF3 Avira P 1 7 8 %windir%\system32\ CFTM.EXE 18 941,200
99167824.EXE 18 941,200
CFTM.EXE 18 941,200
62177957.EXE 18 941,200
CSRCS.EXE 18 941,200
CSRCS.EXE 18 941,200
%programfiles%\emule CFFKQO.EXE 18 941,200
%documents%\ CFFKQO.EXE 18 941,200
?:\sto sigeen websi CFFKQO.EXE 18 941,200

Fig. 11



Value	Key	QuerySet				Key	DataBase			
V:REGRUNSVC\S,REGWINLOG\S,REGEXPLOADS,		38	1,212		0		39	1,209		0
V:REGWINLOG\S,REGEXPLOAD\S,		11	359		0		14	405		0
V:REGRUNSVC\S,REGEXPLOAD\S,		7	185		0		7	189		0
V:REGRUNSVC\S,REGWINLOG\S,REGEXPLOADS,		0	66		0		7	84		0
V:REGEXPLOAD\S,		0	54		0		58	494		4
V:REGRUNSVC\S,		1	19		0		15	69		3
V:REGRUNSVC\S,REGWINLOG\S,		0	12		0		0	12		0
V:REGSESSMGR\S,		0	2		0		1,802	874		1,098

Fig. 12

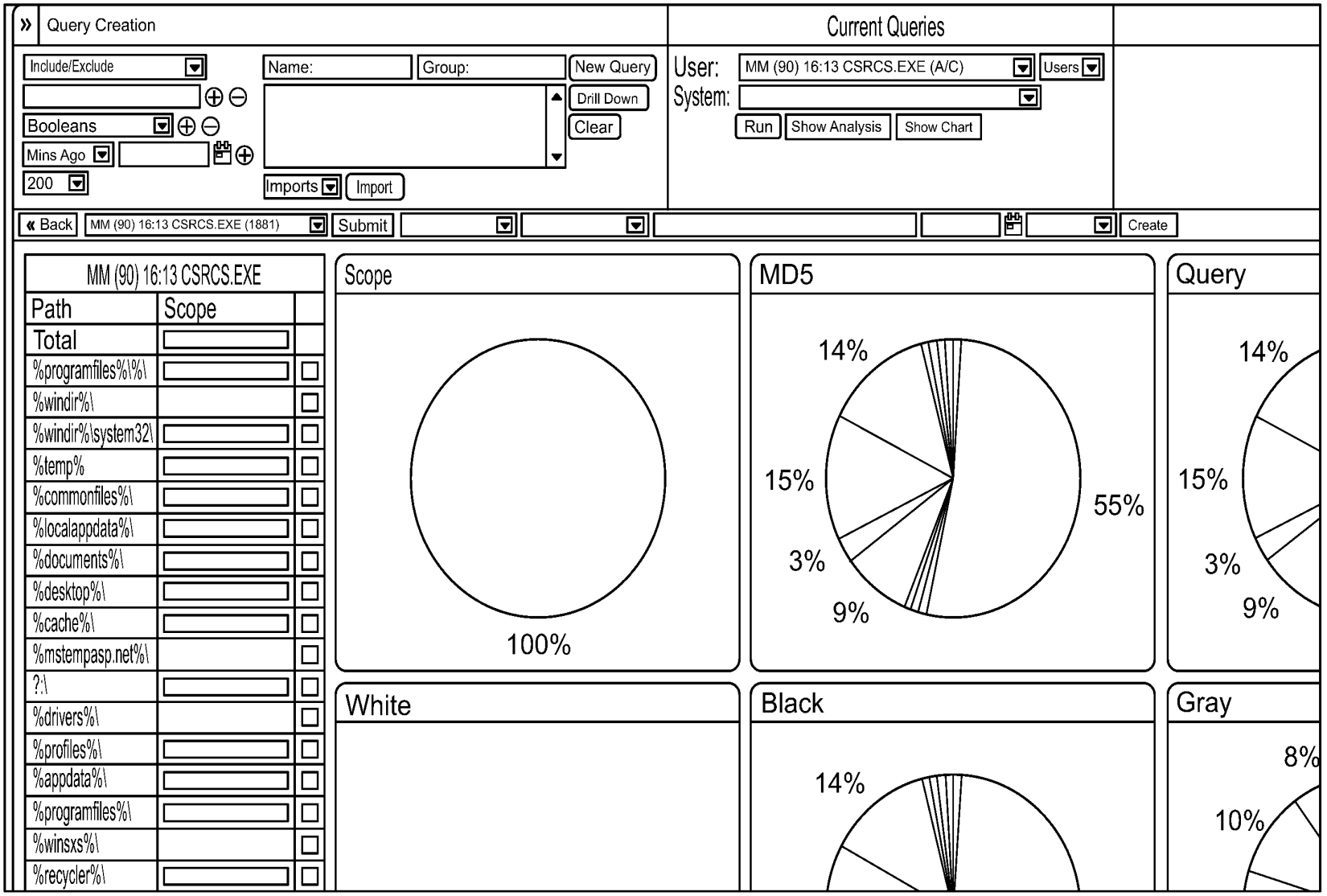

Query Creation
Current Queries
Include/Exclude
Name:
Group:
New Query
Drill Down
Clear
Booleans
Mins Ago
200
Imports
Import
User:
MM (90) 16:13 CSRCS.EXE (A/C)
Users
System:
Run
Show Analysis
Show Chart
« Back
MM (90) 16:13 CSRCS.EXE (1881)
Submit
Create
MM (90) 16:13 CSRCS.EXE
Path
Scope
Total
%programfiles%\%\
%windir%\
%windir%\system32\
%temp%
%commonfiles%\
%localappdata%\
%documents%\
%desktop%\
%cache%\
%mstempasp.net%\
?:\
%drivers%\
%profiles%\
%appdata%\
%programfiles%\
%winsxs%\
%recycler%\
Scope
100%
MD5
14%
15%
55%
3%
9%
Query
14%
15%
3%
9%
White
Black
14%
Gray
8%
10%

Fig. 13

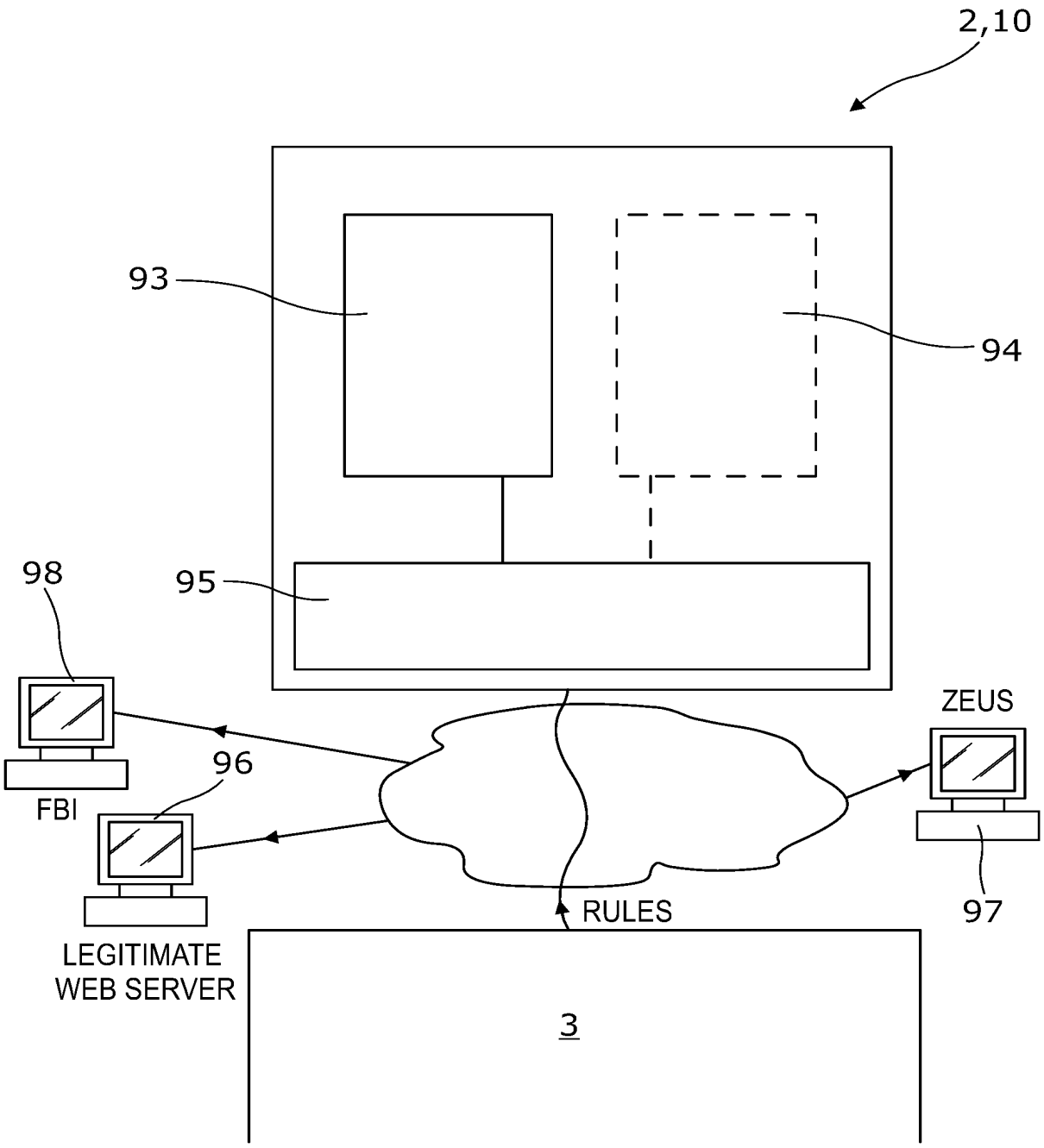


Fig. 14

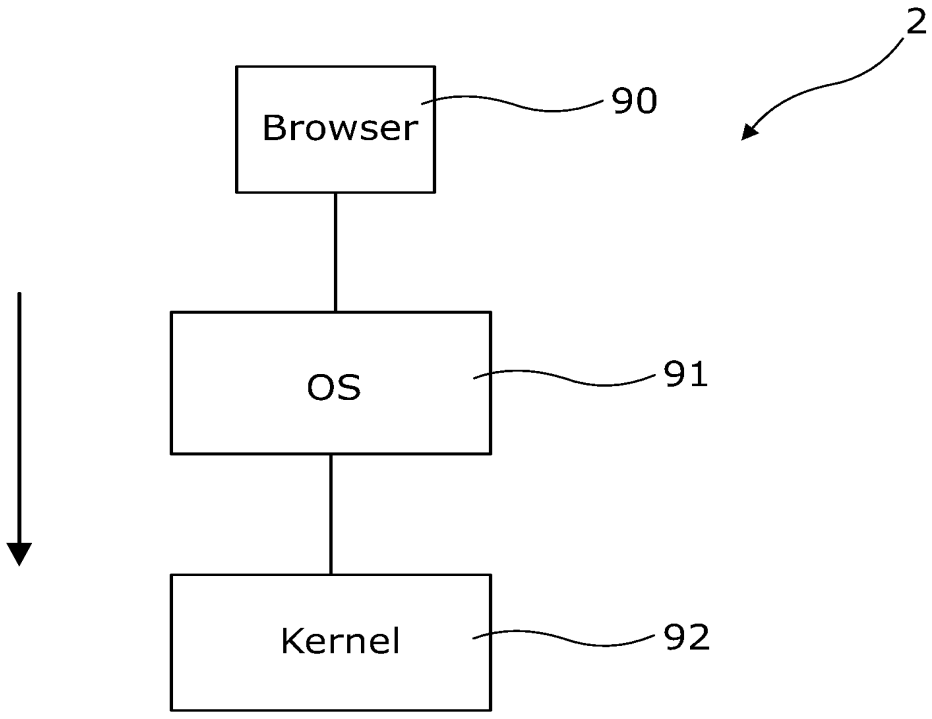


Fig. 15

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2012/052497

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/00
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2007/016953 A1 (MORRIS MELVYN [GB] ET AL) 18 January 2007 (2007-01-18) cited in the application paragraph [0001] - paragraph [0144] -----	1-25, 31-35
A	EP 1 315 066 A1 (BRITISH TELECOMM [GB]) 28 May 2003 (2003-05-28) the whole document -----	1-25, 31-35
X	US 2006/080637 A1 (TREIT RANDAL P [US] ET AL) 13 April 2006 (2006-04-13) paragraph [0008] - paragraph [0012] paragraph [0018] - paragraph [0034] ----- -/--	21, 26-31, 36-40

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
29 June 2012	13/07/2012

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Pinto, Raúl

3

Form PCT/ISA/210 (second sheet) (April 2005)

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2007/220043 A1 (OLIVER IAN [AU] ET AL) 20 September 2007 (2007-09-20) paragraph [0013] - paragraph [0235] -----	21, 26-31, 36-40
X	US 2005/187740 A1 (MARINESCU ADRIAN M [US]) 25 August 2005 (2005-08-25) paragraph [0009] - paragraph [0012] paragraph [0022] - paragraph [0057] -----	41,42
X	US 2009/089040 A1 (MONASTYRSKY ALEXEY V [RU] ET AL) 2 April 2009 (2009-04-02) paragraph [0004] - paragraph [0014] paragraph [0023] - paragraph [0046] -----	41,42
X	Raghunathan Srinivasan: "PROTECTING ANTI-VIRUS SOFTWARE UNDER VIRAL ATTACKS", Arizona State University , August 2007 (2007-08), XP002678947, Retrieved from the Internet: URL:http://www.public.asu.edu/~rsriniv8/Documents/Raghunathan_MS_thesis.pdf [retrieved on 2012-06-29] Chapter 5 -----	43-47
A	Bryce Cogswell and Mark Russinovich: "Rootkit Revealer v1.71", , 1 November 2006 (2006-11-01), XP002678948, Retrieved from the Internet: URL:http://technet.microsoft.com/en-us/sysinternals/bb897445.aspx [retrieved on 2012-06-29] First 2 paragraphs of main text. -----	43-47
X	US 6 175 869 B1 (AHUJA SUDHIR RAMAN [US] ET AL) 16 January 2001 (2001-01-16) column 2, line 15 - column 3, line 20 column 3, line 45 - column 12, line 59 -----	48-56
X	US 2007/174429 A1 (MAZZAFERRI RICHARD JAMES [AU] ET AL) 26 July 2007 (2007-07-26) paragraph [0007] - paragraph [0023] paragraph [0184] paragraph [1163] - paragraph [1166] -----	48-56
X	US 2008/148381 A1 (AARON JEFFREY [US]) 19 June 2008 (2008-06-19) paragraph [0005] - paragraph [0011] paragraph [0015] - paragraph [0047] ----- -/--	57-62

3

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2008/115190 A1 (AARON JEFFREY [US]) 15 May 2008 (2008-05-15) paragraph [0006] - paragraph [0014] paragraph [0020] - paragraph [0055] -----	57-62
A	US 2006/272020 A1 (GARDNER PHILIP B [US]) 30 November 2006 (2006-11-30) the whole document -----	57-62

3

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2012/052497

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2007016953 A1	18-01-2007	CN 101213555 A	02-07-2008
		CN 102096784 A	15-06-2011
		CN 102176224 A	07-09-2011
		EP 1899884 A2	19-03-2008
		JP 2009500706 A	08-01-2009
		US 2007016953 A1	18-01-2007
		WO 2007003916 A2	11-01-2007
EP 1315066 A1	28-05-2003	CA 2467186 A1	05-06-2003
		EP 1315066 A1	28-05-2003
		EP 1446709 A1	18-08-2004
		US 2005022014 A1	27-01-2005
		WO 03046699 A1	05-06-2003
US 2006080637 A1	13-04-2006	NONE	
US 2007220043 A1	20-09-2007	NONE	
US 2005187740 A1	25-08-2005	US 2005187740 A1	25-08-2005
		US 2008141286 A1	12-06-2008
US 2009089040 A1	02-04-2009	US 2009089040 A1	02-04-2009
		US 2009089878 A1	02-04-2009
		US 2009126015 A1	14-05-2009
		US 2009126016 A1	14-05-2009
US 6175869 B1	16-01-2001	NONE	
US 2007174429 A1	26-07-2007	CN 101410803 A	15-04-2009
		US 2007171921 A1	26-07-2007
		US 2007174410 A1	26-07-2007
		US 2007174429 A1	26-07-2007
		US 2007179955 A1	02-08-2007
		US 2007180447 A1	02-08-2007
		US 2007180448 A1	02-08-2007
		US 2007180449 A1	02-08-2007
		US 2007180450 A1	02-08-2007
		US 2007180493 A1	02-08-2007
		US 2007186212 A1	09-08-2007
		US 2007192329 A1	16-08-2007
		US 2007198656 A1	23-08-2007
US 2008148381 A1	19-06-2008	NONE	
US 2008115190 A1	15-05-2008	NONE	
US 2006272020 A1	30-11-2006	NONE	

INTERNATIONAL SEARCH REPORT

International application No.
PCT/EP2012/052497

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☒ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-25, 31-35

   Classifying a computer object as malware

   ---

2. claims: 21, 26-31, 36-40

   Identifying malware based on rules

   ---

3. claims: 41, 42

   Monitoring objects running on a computer

   ---

4. claims: 43-47

   Operating security program on computer

   ---

5. claims: 48-56

   Connecting remote computer to a server

   ---

6. claims: 57-62

   Protecting network against malware

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY
(Chapter I of the Patent Cooperation Treaty)

(PCT Rule 44*bis*)

Applicant's or agent's file reference 6890-103-PCT	**FOR FURTHER ACTION**	See item 4 below
International application No. PCT/US2014/036832	International filing date *(day/month/year)* 05 May 2014 (05.05.2014)	Priority date *(day/month/year)* 03 May 2013 (03.05.2013)
International Patent Classification (8th edition unless older edition indicated) See relevant information in Form PCT/ISA/237		
Applicant WEBROOT INC.		

1. This international preliminary report on patentability (Chapter I) is issued by the International Bureau on behalf of the International Searching Authority under Rule 44 *bis*.1(a).

2. This REPORT consists of a total of 8 sheets, including this cover sheet.

   In the attached sheets, any reference to the written opinion of the International Searching Authority should be read as a reference to the international preliminary report on patentability (Chapter I) instead.

3. This report contains indications relating to the following items:

☒	Box No. I	Basis of the report
☐	Box No. II	Priority
☐	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
☐	Box No. IV	Lack of unity of invention
☒	Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
☐	Box No. VI	Certain documents cited
☐	Box No. VII	Certain defects in the international application
☐	Box No. VIII	Certain observations on the international application

4. The International Bureau will communicate this report to designated Offices in accordance with Rules 44*bis*.3(c) and 93*bis*.1 but not, except where the applicant makes an express request under Article 23(2), before the expiration of 30 months from the priority date (Rule 44*bis* .2).

	Date of issuance of this report 03 November 2015 (03.11.2015)
The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No. +41 22 338 82 70	Authorized officer Agnès Wittmann-Regis e-mail: pt06.pct@wipo.int

Form PCT/IB/373 (January 2004)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To: BRENT R. LINDON
SHERIDAN ROSS P.C.
1560 BROADWAY
SUITE 1200
DENVER, CO 80202

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)*	29 SEP 2014
Applicant's or agent's file reference 6890-103-PCT	**FOR FURTHER ACTION** See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2014/036832	05 May 2014	03 May 2013

International Patent Classification (IPC) or both national classification and IPC
IPC(8) - G06F21/00 (2014.01)
CPC - H04L63/14 (2014.02)

Applicant WEBROOT INC.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1 *bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA/US	Date of completion of this opinion	Authorized officer:
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	09 September 2014	Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/237 (cover sheet) (July 2011)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2014/036832

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed.

   ☐ a translation of the international application into _____ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing filed or furnished:

   a. (means)

   ☐ on paper

   ☐ in electronic form

   b. (time)

   ☐ in the international application as filed

   ☐ together with the international application in electronic form

   ☐ subsequently to this Authority for the purposes of search

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2014/036832

Box No. V **Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	5-7, 14-16, 19-20	YES
	Claims	1-4, 8-13, 17-18	NO
Inventive step (IS)	Claims	None	YES
	Claims	1-20	NO
Industrial applicability (IA)	Claims	1-20	YES
	Claims	None	NO

2. Citations and explanations:

Claims 1-4, 8-13 and 17-18 lack novelty under PCT Article 33(2) as being anticipated by Morris et al. (hereinafter Morris).

Regarding claim 1, Morris teaches a method (abstract) comprising: gathering one or more events defining an action of a first object acting on a target (para [0056] discloses an agent program running on a remote computer searches a local database for information related to events, where, as further disclosed in para [0056], events define the actions or behaviors of an object acting upon another object. The event includes the key of the object performing the act [claimed first object] and the identity of another object which the act is being performed on [claimed target]); generating a contextual state for at least one of the one or more events by correlating the at least one event to an originating object (para [0055], discloses generating metadata [claimed contextual state], where, as further disclosed in para [0058], the metadata includes Genesisactor information which includes the parent of the object being performed [claimed originating object]. For example in the case of a software installation, this would be the key of the object that the user or system first executed and that initiated the software installation process, e.g. Setup.exe), the contextual state including an indication of the originating object of the first object (para [0058], the metadata includes Genesisactor information which includes the parent of the object being performed [claimed originating object of the first object]) and an indication of at least one of a device on which the first object is executed and a user associated with the first object (para [0119] discloses metadata may include operating system of the remote computer that encountered the object [claimed indication of a device] and author of the object [claimed user associated with the first object]); obtaining a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object (para [0125], a collective view of the object, i.e. its meta data and behaviors, across all agents that have seen it, provides an informed view [thus, a collective view [claimed global perspective] of the object is established by allowing agents to analyze and share obtained metadata relating to objects]. Further, as disclosed in para [0056] and [0058], the metadata information may include information of the object performing the act [claimed first object], the event type and the parent object [claimed originating object]), the information including at least one of age (pare [0134], objects having a specific determination, location, popularity, age or any other criteria known by or derived by the database), popularity (para [0134]), a determination as to whether the first object is malware (para [0015], determine whether or not the object is malware), a determination as to whether the originating object is malware (determine whether or not the object is malware. Also see para [0058]); and Internet Protocol (IP) Address or Uniform Resource Locator (URL) information (para [0056], the IP address or URL); assembling an event line including details associated with the at least one event, the details including information uniquely identifying each of the first object (para [0046], the details of an object that are passed to the base computer may be in the form of a signature or "key" that uniquely identifies the object), the action of the first object (para [0055]-0056], metadata details captured and sent include events, which define the actions or behaviors of an object), the target (para [0056], victim), and the originating object (para [0058], parent object); and transmitting the assembled event line (para [0046], The details of an object that are passed [claimed transmitting] to the base computer. Further, as disclosed in para [0055], metadata details are passed [claimed transmitting] to the base computer.).

Regarding claim 2, Morris teaches wherein the information associated with the one or more of the first object and the originating object is obtained from a community database (para [0061], community database of metadata information); and wherein the event line is transmitted to an end recipient (para [0125], collected metadata can be retrieved by a human [claimed end recipient]).

Regarding claim 3, Morris teaches obtaining an event priority based on one or more of the generated context and the global perspective for the at least one event (para [0061] discloses generating rules using metadata [claimed context] received from remote computers, where as further disclosed in para [0056], the metadata includes event information. Further, as disclosed in para [0134], rules may be prioritized and applied against objects with specific metadata [the prioritized rules are based on specific metadata [claimed context], which include event information, thus a specific event an associated priority]), wherein the event line further includes the event priority for the at least one event (para [0134] discloses associating a prioritized rule with metadata information, where, as further disclosed in para [0056], the metadata information includes event information. Further, as disclosed in para [0061], the database creates stores and transmits details of the rules [claimed event line] to be applied by the remote computers [thus, the database maintains details [claimed event line] of the prioritized rules associated with the monitored events]).

Regarding claim 4, Morris teaches wherein the at least one event includes information uniquely identifying the object performing the action (para [0056], the event includes information of the object performing the act), information uniquely identifying the action being performed (para [0056], the event includes information of the act being performed), and information uniquely identifying the target upon which the act is being performed (para [0056], the event includes the object or identity of another entity upon which the act is being performed).

Regarding claim 8, Morris teaches a computer readable storage medium comprising processor executable 20 instructions operable to perform the method of claim 1 (para [0156]-[0157]).

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2014/036832

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:

Regarding claims 9 and 17, Morris teaches a system for providing forensic visibility into a system (para [0142], forensic data handling), comprising: a device including: a communication interface; a processor; data storage; and a sensor agent stored on the data storage that is executable by the processor (para [0018], agent program [claimed sensor agent] installed on a remote computer [claimed device]. Also see para [0156]), wherein the sensor agent is operable to: (para [0056] discloses an agent program running on a remote computer searches a local database for information related to events, where, as further disclosed in para [0056], events define the actions or behaviors of an object acting upon another object. The event includes the key of the object performing the act [claimed first object] and the identity of another object which the act is being performed on [claimed target]); generating a contextual state for at least one of the one or more events by correlating the at least one event to an originating object (para [0055], discloses generating metadata [claimed contextual state], where, as further disclosed in para [0058], the metadata includes Genesisactor information which includes the parent of the object being performed [claimed originating object]. For example in the case of a software installation, this would be the key of the object that the user or system first executed and that initiated the software installation process, e.g. Setup.exe), the contextual state including an indication of the originating object of the first object (para [0058], the metadata includes Genesisactor information which includes the parent of the object being performed [claimed originating object of the first object]) and an indication of at least one of a device on which the first object is executed and a user associated with the first object (para [0119] discloses metadata may include operating system of the remote computer that encountered the object [claimed indication of a device] and author of the object [claimed user associated with the first object]); obtaining a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object (para [0125], a collective view of the object, i.e. its meta data and behaviors, across all agents that have seen it, provides an informed view [thus, a collective view [claimed global perspective] of the object is established by allowing agents to analyze and share obtained metadata relating to objects]. Further, as disclosed in para [0056] and [0058], the metadata information may include information of the object performing the act [claimed first object], the event type and the parent object [claimed originating object]), the information including at least one of age (pare [0134], objects having a specific determination, location, popularity, age or any other criteria known by or derived by the database), popularity (para [0134]), a determination as to whether the first object is malware (para [0015], determine whether or not the object is malware), a determination as to whether the originating object is malware (determine whether or not the object is malware. Also see para [0058]); and Internet Protocol (IP) Address or Uniform Resource Locator (URL) information (para [0056], the IP address or URL); assembling an event line including details associated with the at least one event, the details including information uniquely identifying each of the first object (para [0046], the details of an object that are passed to the base computer may be in the form of a signature or "key" that uniquely identifies the object), the action of the first object (para [0055]-0056], metadata details captured and sent include events, which define the actions or behaviors of an object), the target (para [0056], victim), and the originating object (para [0058], parent object); and transmitting the assembled event line utilizing the communication interface (para [0046], The details of an object that are passed [claimed transmitting] to the base computer. Further, as disclosed in para [0055], metadata details are passed [claimed transmitting] to the base computer, where, as further disclosed in para [0061], the metadata information is derived from the remote computers [thus, the remote computers, which includes the agent program, will send the metadata information through an associated interface]. Also see para [0014]).

Regarding claim 10, Morris teaches wherein the at least one of the one or more events is executed by the processor (para [0156]).

Regarding claim 11, Morris teaches a global perspective information server (para [0073], ENZO central servers that aggregate all of the collected data); and an end recipient device (para [0125], human access collected data), wherein the information associated with the one or more of the first object and the originating object is obtained from the global perspective information server (para [0091] discloses the ENZO server propagates metadata information to remote computers, where, as further disclosed in para [0056] and [0058], the metadata information may include information of the object performing the act [claimed first object] and the parent object [claimed originating object]) and the sensor agent transmits the event line to the end recipient (para [0055], metadata details are passed [claimed transmitting] to the base computer, where, as further disclosed in para [0061], the metadata information is derived from the remote computers [thus, the remote computers, which includes the agent program, will send the metadata information through an associated interface]. Also see para [0014]).

Regarding claim 12, Morris teaches wherein the sensor agent is further operable to: cache the one or more events (para [0035], a local agent [claimed sensor agent] of a remote computer searches a local database stored at the remote computer. Further, as disclosed in para [0039], the local database copies the signature information from a community database for retrieval [thus, the information is cached locally for faster retrieval]); and asynchronously consolidate and normalize the one or more events (para [0093], the agent program on the remote computer coordinates with the ENZO server to update metadata information about which objects have been seen by the community so as not to store duplicated metadata, where, as further disclosed in para [0056], the metadata includes event information. Further, as disclosed in para [0093], this process is initiated when the remote computers and the associated agents receive a data packet [thus, each remote computer will initiate the coordination with the ENZO server dynamically and not in a synchronized operation]).

Regarding claim 13, Morris teaches wherein the at least one event includes information uniquely identifying the object performing the action (para [0056], the event includes information of the object performing the act), information uniquely identifying the action being performed (para [0056], the event includes information of the act being performed), and information uniquely identifying the target upon which the act is being performed (para [0056], the event includes the object or identity of another entity upon which the act is being performed).

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2014/036832

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:

Regarding claim 18, Morris teaches a global perspective information server (para [0073], ENZO central servers that aggregate all of the collected data) including: a processor ([0156]); a communication interface (para [0093] discloses the ENZO server communicates with remote computers [thus, the server will have an associated interface]; data storage (para [0093], ENZO server stores metadata information. Also see para [0073]); and a global perspective module, wherein the global perspective module is operable to: receive the event line from the device (para [0073] discloses aggregate all of the information received from all remote computers [thus, the server will have a global perspective of all metadata information]. Also see para [0074]-[0076] and [0093]); obtain a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object (para [0093] discloses the ENZO server stores all metadata information, where, as further disclosed in para [0056] and [0058], the metadata information may include information of the object performing the act [claimed first object] and the parent object [claimed originating object]), the information including at least one of age (pare [0134], objects having a specific determination, location, popularity, age or any other criteria known by or derived by the database), popularity (para [0134]), a determination as to whether the first object is malware (para [0015], determine whether or not the object is malware), a determination as to whether the originating object is malware (determine whether or not the object is malware. Also see para [0058]); and Internet Protocol (IP) Address or Uniform Resource Locator (URL) information (para [0056], the IP address or URL); assemble a second event line including details associated with the at least one event (para [0093] discloses the ENZO server maintains a master list [claimed second event line] of all metadata information and propagates the list to all remote computers), the details including information uniquely identifying each of the first object (para [0056], metadata information includes events related to objects performing the act), the action of the first object (para [0056] discloses metadata information includes the act being performed), the target (para [0056] discloses metadata information includes the victim), and the originating object (para [0058], metadata information includes parent object); and transmit the assembled second event line utilizing the communication interface to an end recipient (para [0093] discloses the ENZO server maintains a master list [claimed second event line] of all metadata information and propagates the list to all remote computers).

Claims 7, 16 and 19 lack an inventive step under PCT Article 33(3) as being obvious over Morris.

Regarding claim 7, Morris teaches heuristically displaying information identifying the first object performing the action (para [0125] discloses displaying the collected information regarding the monitored objects, where, as further disclosed in para [0061], the collected information in the database include rules and heuristics), information identifying the action being performed (para [0056]), information identifying the target upon which the act is being performed (para [0056]), and the global perspective according to one or more of a location associated with the first object (para [0125] discloses obtaining a collective view of an object including its metadata and behaviors, where, as further disclosed in para [0057], the metadata includes location information. Also see para [0119]); at least one characteristic of an outbound connection associated with the first object (para [0056], a network entity with which an object is communicating); a executable file (para [0111], The data can also be measured against their filenames, and file types (e.g. .exe) [claimed executable file]. Also see para [0058]); an age of the first object (para [0044] discloses monitoring a process [claimed object] for a period of n days [claimed age] to determine whether the process is safe. Also see para [0132]); and connections associated with the first object (para [0056], a network entity with which an object is communicating).
Morris does not teach identifying dropped files and a number of concurrent connections. However, configuring management of data and data connections has been a practice well known in the art and the specifics (identifying dropped files and a number of concurrent connections) would have been a matter of design choice. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate identifying dropped files and a number of concurrent connections in the invention of Morris. The motivation do so would have been to enhance the detection of security attacks by collecting and displaying security related information (Morris, para [0125]).

Regarding claim 16, Morris teaches heuristically displaying information identifying the first object performing the action (para [0125] discloses displaying the collected information regarding the monitored objects, where, as further disclosed in para [0061], the collected information in the database include rules and heuristics), information identifying the action being performed (para [0056]), information identifying the target upon which the act is being performed (para [0056]), and the global perspective according to one or more of a location associated with the first object (para [0125] discloses obtaining a collective view of an object including its metadata and behaviors, where, as further disclosed in para [0057], the metadata includes location information. Also see para [0119]); at least one characteristic of an outbound connection associated with the first object (para [0056], a network entity with which an object is communicating); a executable file (para [0111], The data can also be measured against their filenames, and file types (e.g. .exe) [claimed executable file]. Also see para [0058]); an age of the first object (para [0044] discloses monitoring a process [claimed object] for a period of n days [claimed age] to determine whether the process is safe. Also see para [0132]); and connections associated with the first object (para [0056], a network entity with which an object is communicating).
Morris does not teach identifying dropped files and a number of concurrent connections. However, configuring management of data and data connections has been a practice well known in the art and the specifics (identifying dropped files and a number of concurrent connections) would have been a matter of design choice. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate identifying dropped files and a number of concurrent connections in the invention of Morris. The motivation do so would have been to enhance the detection of security attacks by collecting and displaying security related information (Morris, para [0125]).

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No. PCT/US2014/036832

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:

Regarding claim 19, Morris teaches wherein the end recipient heuristically displays information identifying the first object performing the action (para [0125] discloses displaying the collected information regarding the monitored objects, where, as further disclosed in para [0061], the collected information in the database include rules and heuristics), information identifying the action being performed (para [0056]), information identifying the target upon which the act is being performed (para [0056]), and the global perspective according to one or more of a location associated with the first object (para [0125] discloses obtaining a collective view of an object including its metadata and behaviors, where, as further disclosed in para [0057], the metadata includes location information. Also see para [0119]); at least one characteristic of an outbound connection associated with the first object (para [0056], a network entity with which an object is communicating); a executable file (para [0111], The data can also be measured against their filenames, and file types (e.g. .exe) [claimed executable file]. Also see para [0058]); an age of the first object (para [0044] discloses monitoring a process [claimed object] for a period of n days [claimed age] to determine whether the process is safe. Also see para [0132]); and connections associated with the first object (para [0056], a network entity with which an object is communicating).
Morris does not teach identifying dropped files and a number of concurrent connections. However, configuring management of data and data connections has been a practice well known in the art and the specifics (identifying dropped files and a number of concurrent connections) would have been a matter of design choice. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate identifying dropped files and a number of concurrent connections in the invention of Morris. The motivation do so would have been to enhance the detection of security attacks by collecting and displaying security related information (Morris, para [0125]).

Claims 5-6 and 14-15 lack an inventive step under PCT Article 33(3) as being obvious over Morris in view of Crosby et al (hereinafter Crosby).

Regarding claim 5, Morris teaches determining whether [information] for the at least one event has been cached (para [0035], search a local database stored at the remote computer to search for a signature or key representing that particular process, its related objects and/or the event. Further, as disclosed in para [0039], the local database copies the signature information from a community database for retrieval [thus, the information is cached locally for faster retrieval]); when the [information] for the at least one event has been cached, obtaining [information] for the at least one event based on the cached information (para [0035], If the local signature is present, it will indicate either that the process is considered to be safe or will indicate that that process is considered unsafe [claimed obtaining information based on the stored information]);
and when the [information] for the at least one event has not been cached, obtaining [information] for the at least one event from a community database (para [0039], when a local signature is not found, a community database is searched and used to retrieve the required signature information which is sent to the local computer).
Morris does not teach caching a global perspective. However, Crosby, in analogous art, teaches monitoring security attacks (abstract). Crosby further teaches caching a global perspective (para [0042] discloses a locally storing global beliefs [claimed global perspective] regarding the security state of the system. Also see para [0023] and [0025]). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Crosby to incorporate caching a global perspective in the invention of Morris in order to enhance detection of security attacks (Crosby, para [0042]).

Regarding claim 6, Morris teaches obtaining [information] for the at least one event from a community database (para [0039]).
Morris does not teach determining whether the cached global perspective for the at least one event has expired; and when the global perspective for the at least one event has expired, obtaining a global perspective for the at least one event from a database.
However Crosby, in analogous art, teaches determining whether the cached global perspective for the at least one event has expired (para [0043] discloses whether global beliefs are older than a maximum age value [claimed expired]); and when the global perspective for the at least one event has expired (para [0043], determine whether global belief has exceeded maximum age. Also see para [0023]).
Furthermore, configuring management of data has been a practice well known in the art and the specifics (obtaining a global perspective from a database when the global perspective has expired) would have been a matter of design choice. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Crosby to incorporate retrieval of information from a database when the information has expired in the invention of Morris in order to enhance the detection of new security attacks (Crosby, para [0043]).

Regarding claim 14, Morris teaches determining whether [information] for the at least one event has been cached (para [0035], search a local database stored at the remote computer to search for a signature or key representing that particular process, its related objects and/or the event. Further, as disclosed in para [0039], the local database copies the signature information from a community database for retrieval [thus, the information is cached locally for faster retrieval]);
when the [information] for the at least one event has been cached, obtaining [information] for the at least one event based on the cached information (para [0035], If the local signature is present, it will indicate either that the process is considered to be safe or will indicate that that process is considered unsafe [claimed obtaining information based on the stored information]);
and when the [information] for the at least one event has not been cached, obtaining [information] for the at least one event from a community database (para [0039], when a local signature is not found, a community database is searched and used to retrieve the required signature information which is sent to the local computer).
Morris does not teach caching a global perspective. However, Crosby, in analogous art, teaches monitoring security attacks (abstract). Crosby further teaches caching a global perspective (para [0042] discloses a locally storing global beliefs [claimed global perspective] regarding the security state of the system. Also see para [0023] and [0025]). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Crosby to incorporate caching a global perspective in the invention of Morris in order to enhance detection of security attacks (Crosby, para [0042]).

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2014/036832

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:

Regarding claim 15, Morris teaches obtaining [information] for the at least one event from a community database (para [0039]). Morris does not teach determining whether the cached global perspective for the at least one event has expired; and when the global perspective for the at least one event has expired, obtaining a global perspective for the at least one event from a database. However Crosby, in analogous art, teaches determining whether the cached global perspective for the at least one event has expired (para [0043] discloses whether global beliefs are older than a maximum age value [claimed expired]); and when the global perspective for the at least one event has expired (para [0043], determine whether global belief has exceeded maximum age. Also see para [0023]). Furthermore, configuring management of data has been a practice well known in the art and the specifics (obtaining a global perspective from a database when the global perspective has expired) would have been a matter of design choice. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Crosby to incorporate retrieval of information from a database when the information has expired in the invention of Morris in order to enhance the detection of new security attacks (Crosby, para [0043]).

Claims 20 lack an inventive step under PCT Article 33(3) as being obvious over Morris in view of Fanton et al. (hereinafter Fanton)

Regarding claim 20, Morris teaches a bridge (para [0035], local database) including: a processor (para [0156]); a communication interface (para [0065], the agent program communicates with the local database [thus, the local database will have an associated interface to communicate]; and a cached event store (para [0065], local database holds a local copy [claimed cache]of signatures relating to the objects found on the remote computer), wherein the cached event store is operable to: receive a first request for [information] for the at least one event (para [0035], the local database is searched for signature or key representing a process, its related objects and/or event); receive a second request for a [information] for another event (para [0035] discloses searching a local database to determine whether a monitored object is safe or unsafe [thus, for each new monitored object received at the remote computer, a local database will be searched for associated information regarding the object and its related events]), obtain a first [information] for the at least one event by obtaining information associated with one or more of the first object and the originating object (para [0034]-[0035] discloses searching a local database for metadata information, where, as further disclosed in para [0056] and [0058], the metadata information may include information of the object performing the act [claimed first object] and the parent object [claimed originating object]), the information including at least one of pare [0134], objects having a specific determination, location, popularity, age or any other criteria known by or derived by the database), popularity (para [0134]), a determination as to whether the first object is malware (para [0015], determine whether or not the object is malware), a determination as to whether the originating object is malware (determine whether or not the object is malware. Also see para [0058]); and Internet Protocol (IP) Address or Uniform Resource Locator (URL) information (para [0056], the IP address or URL); obtain a second [information] for the another event (para [0035] discloses searching a local database to determine whether a monitored object is safe or unsafe [thus, for each new monitored object received at the remote computer, a local database will be searched for associated information regarding the object and its related events]); provide the first [information] to the device (para [0035]);
Morris does not teach receive a request for global perspective, a second request for a global perspective from another device, provide the first global perspective to the first device and the second global perspective to the another device. However, Fanton, in analogous art, teaches protecting a computer system from attack (para [0022]). Fanton further teaches receive a request for global perspective, a second request for a global perspective from another device, provide the first global perspective to the first device and the second global perspective to the another device (para [0009] discloses generating and searching [claimed request] a global white list [claimed global perspective] to determine if a program is safe to run, where, as further disclosed in para [0039], the global white list may be maintained in a server for an enterprise network to provide a group wide policy [thus, a first and second end user of the enterprise will search a global white list stored on the server to receive a determination on the end user device to run the program]). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Fanton to incorporate send global perspective information to a first and second device in the invention of Morris in order to enhance the security of enterprise networks (Fanton, para [0039]).

Claims 1-20 meet the criteria set out in PCT Article 33(4), and thus have industrial applicability because the subject matter claimed can be made or used in industry.

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference 6890-103-PCT	**FOR FURTHER ACTION**	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
International application No. PCT/US2014/036832	International filing date *(day/month/year)* 05 May 2014	(Earliest) Priority Date *(day/month/year)* 03 May 2013
Applicant WEBROOT INC.		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 2 sheets.

☐ It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**

a. With regard to the **language**, the international search was carried out on the basis of:

☒ the international application in the language in which it was filed.

☐ a translation of the international application into _____ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

b. ☐ This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6*bis*(a)).

c. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2. ☐ **Certain claims were found unsearchable** (see Box No. II).

3. ☐ **Unity of invention is lacking** (see Box No. III).

4. With regard to the **title**,

☒ the text is approved as submitted by the applicant.

☐ the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,

☒ the text is approved as submitted by the applicant.

☐ the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the **drawings**,

a. the figure of the **drawings** to be published with the abstract is Figure No. 2

☒ as suggested by the applicant.

☐ as selected by this Authority, because the applicant failed to suggest a figure.

☐ as selected by this Authority, because this figure better characterizes the invention.

b. ☐ none of the figures is to be published with the abstract.

Form PCT/ISA/210 (first sheet) (July 2009)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2014/036832

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06F21/00 (2014.01)
CPC - H04L63/14 (2014.02)
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC(8) - G06F21/00; G06F12/14; G06F11/30; H04L9/32 (2014.01)
USPC - 709/224; 726/22, 23, 25

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
CPC - H04L63/14; H04L63/1408; H04L63/1416; H04L63/1425 (2014.02)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
PatBase, Google Patents, Google Scholar

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 2012/0260340 A1 (MORRIS et al.) 11 October 2012 (11.10.2012) entire document	1-4, 7-13, 16-19 --- 5-6, 14-15, 20
Y	US 2006/0095963 A1 (CROSBY et al.) 04 May 2006 (04.05.2006) entire document	5-6, 14-15
Y	US 2012/0072725 A1 (FANTON et al.) 22 March 2012 (22.03.2012) entire document	20
A	US 7,895,649 B1 (BROOK et al.) 22 February 2011 (22.02.2011) entire document	1-20
A	US 2009/0300769 A1 (SRINIVASA et al.) 03 December 2009 (03.12.2009) entire document	1-20

☐ Further documents are listed in the continuation of Box C. ☐

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
09 September 2014	29 SEP 2014
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (July 2009)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To: BRENT R. LINDON
SHERIDAN ROSS P.C.
1560 BROADWAY
SUITE 1200
DENVER, CO 80202

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)*	29 SEP 2014
Applicant's or agent's file reference 6890-103-PCT	**FOR FURTHER ACTION** See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2014/036832	05 May 2014	03 May 2013

International Patent Classification (IPC) or both national classification and IPC
IPC(8) - G06F21/00 (2014.01)
CPC - H04L63/14 (2014.02)

Applicant WEBROOT INC.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1 *bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Fom PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA/US	Date of completion of this opinion	Authorized officer:
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	09 September 2014	Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/237 (cover sheet) (July 2011)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2014/036832

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed.

   ☐ a translation of the international application into _____ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing filed or furnished:

   a. (means)

   ☐ on paper

   ☐ in electronic form

   b. (time)

   ☐ in the international application as filed

   ☐ together with the international application in electronic form

   ☐ subsequently to this Authority for the purposes of search

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2014/036832

Box No. V **Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	5-7, 14-16, 19-20	YES
	Claims	1-4, 8-13, 17-18	NO
Inventive step (IS)	Claims	None	YES
	Claims	1-20	NO
Industrial applicability (IA)	Claims	1-20	YES
	Claims	None	NO

2. Citations and explanations:

Claims 1-4, 8-13 and 17-18 lack novelty under PCT Article 33(2) as being anticipated by Morris et al. (hereinafter Morris).

Regarding claim 1, Morris teaches a method (abstract) comprising: gathering one or more events defining an action of a first object acting on a target (para [0056] discloses an agent program running on a remote computer searches a local database for information related to events, where, as further disclosed in para [0056], events define the actions or behaviors of an object acting upon another object. The event includes the key of the object performing the act [claimed first object] and the identity of another object which the act is being performed on [claimed target]); generating a contextual state for at least one of the one or more events by correlating the at least one event to an originating object (para [0055], discloses generating metadata [claimed contextual state], where, as further disclosed in para [0058], the metadata includes Genesisactor information which includes the parent of the object being performed [claimed originating object]. For example in the case of a software installation, this would be the key of the object that the user or system first executed and that initiated the software installation process, e.g. Setup.exe), the contextual state including an indication of the originating object of the first object (para [0058], the metadata includes Genesisactor information which includes the parent of the object being performed [claimed originating object of the first object]) and an indication of at least one of a device on which the first object is executed and a user associated with the first object (para [0119] discloses metadata may include operating system of the remote computer that encountered the object [claimed indication of a device] and author of the object [claimed user associated with the first object]); obtaining a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object (para [0125], a collective view of the object, i.e. its meta data and behaviors, across all agents that have seen it, provides an informed view [thus, a collective view [claimed global perspective] of the object is established by allowing agents to analyze and share obtained metadata relating to objects]. Further, as disclosed in para [0056] and [0058], the metadata information may include information of the object performing the act [claimed first object], the event type and the parent object [claimed originating object]), the information including at least one of age (pare [0134], objects having a specific determination, location, popularity, age or any other criteria known by or derived by the database), popularity (para [0134]), a determination as to whether the first object is malware (para [0015], determine whether or not the object is malware), a determination as to whether the originating object is malware (determine whether or not the object is malware. Also see para [0058]); and Internet Protocol (IP) Address or Uniform Resource Locator (URL) information (para [0056], the IP address or URL); assembling an event line including details associated with the at least one event, the details including information uniquely identifying each of the first object (para [0046], the details of an object that are passed to the base computer may be in the form of a signature or "key" that uniquely identifies the object), the action of the first object (para [0055]-0056], metadata details captured and sent include events, which define the actions or behaviors of an object), the target (para [0056], victim), and the originating object (para [0058], parent object); and transmitting the assembled event line (para [0046], The details of an object that are passed [claimed transmitting] to the base computer. Further, as disclosed in para [0055], metadata details are passed [claimed transmitting] to the base computer.).

Regarding claim 2, Morris teaches wherein the information associated with the one or more of the first object and the originating object is obtained from a community database (para [0061], community database of metadata information); and wherein the event line is transmitted to an end recipient (para [0125], collected metadata can be retrieved by a human [claimed end recipient]).

Regarding claim 3, Morris teaches obtaining an event priority based on one or more of the generated context and the global perspective for the at least one event (para [0061] discloses generating rules using metadata [claimed context] received from remote computers, where as further disclosed in para [0056], the metadata includes event information. Further, as disclosed in para [0134], rules may be prioritized and applied against objects with specific metadata [the prioritized rules are based on specific metadata [claimed context], which include event information, thus a specific event an associated priority]), wherein the event line further includes the event priority for the at least one event (para [0134] discloses associating a prioritized rule with metadata information, where, as further disclosed in para [0056], the metadata information includes event information. Further, as disclosed in para [0061], the database creates stores and transmits details of the rules [claimed event line] to be applied by the remote computers [thus, the database maintains details [claimed event line] of the prioritized rules associated with the monitored events]).

Regarding claim 4, Morris teaches wherein the at least one event includes information uniquely identifying the object performing the action (para [0056], the event includes information of the object performing the act), information uniquely identifying the action being performed (para [0056], the event includes information of the act being performed), and information uniquely identifying the target upon which the act is being performed (para [0056], the event includes the object or identity of another entity upon which the act is being performed).

Regarding claim 8, Morris teaches a computer readable storage medium comprising processor executable 20 instructions operable to perform the method of claim 1 (para [0156]-[0157]).

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2014/036832

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:

Regarding claims 9 and 17, Morris teaches a system for providing forensic visibility into a system (para [0142], forensic data handling), comprising: a device including: a communication interface; a processor; data storage; and a sensor agent stored on the data storage that is executable by the processor (para [0018], agent program [claimed sensor agent] installed on a remote computer [claimed device]. Also see para [0156]), wherein the sensor agent is operable to: (para [0056] discloses an agent program running on a remote computer searches a local database for information related to events, where, as further disclosed in para [0056], events define the actions or behaviors of an object acting upon another object. The event includes the key of the object performing the act [claimed first object] and the identity of another object which the act is being performed on [claimed target]); generating a contextual state for at least one of the one or more events by correlating the at least one event to an originating object (para [0055], discloses generating metadata [claimed contextual state], where, as further disclosed in para [0058], the metadata includes Genesisactor information which includes the parent of the object being performed [claimed originating object]. For example in the case of a software installation, this would be the key of the object that the user or system first executed and that initiated the software installation process, e.g. Setup.exe), the contextual state including an indication of the originating object of the first object (para [0058], the metadata includes Genesisactor information which includes the parent of the object being performed [claimed originating object of the first object]) and an indication of at least one of a device on which the first object is executed and a user associated with the first object (para [0119] discloses metadata may include operating system of the remote computer that encountered the object [claimed indication of a device] and author of the object [claimed user associated with the first object]); obtaining a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object (para [0125], a collective view of the object, i.e. its meta data and behaviors, across all agents that have seen it, provides an informed view [thus, a collective view [claimed global perspective] of the object is established by allowing agents to analyze and share obtained metadata relating to objects]. Further, as disclosed in para [0056] and [0058], the metadata information may include information of the object performing the act [claimed first object], the event type and the parent object [claimed originating object]), the information including at least one of age (pare [0134], objects having a specific determination, location, popularity, age or any other criteria known by or derived by the database), popularity (para [0134]), a determination as to whether the first object is malware (para [0015], determine whether or not the object is malware), a determination as to whether the originating object is malware (determine whether or not the object is malware. Also see para [0058]); and Internet Protocol (IP) Address or Uniform Resource Locator (URL) information (para [0056], the IP address or URL); assembling an event line including details associated with the at least one event, the details including information uniquely identifying each of the first object (para [0046], the details of an object that are passed to the base computer may be in the form of a signature or "key" that uniquely identifies the object), the action of the first object (para [0055]-0056], metadata details captured and sent include events, which define the actions or behaviors of an object), the target (para [0056], victim), and the originating object (para [0058], parent object); and transmitting the assembled event line utilizing the communication interface (para [0046], The details of an object that are passed [claimed transmitting] to the base computer. Further, as disclosed in para [0055], metadata details are passed [claimed transmitting] to the base computer, where, as further disclosed in para [0061], the metadata information is derived from the remote computers [thus, the remote computers, which includes the agent program, will send the metadata information through an associated interface]. Also see para [0014]).

Regarding claim 10, Morris teaches wherein the at least one of the one or more events is executed by the processor (para [0156]).

Regarding claim 11, Morris teaches a global perspective information server (para [0073], ENZO central servers that aggregate all of the collected data); and an end recipient device (para [0125], human access collected data), wherein the information associated with the one or more of the first object and the originating object is obtained from the global perspective information server (para [0091] discloses the ENZO server propagates metadata information to remote computers, where, as further disclosed in para [0056] and [0058], the metadata information may include information of the object performing the act [claimed first object] and the parent object [claimed originating object]) and the sensor agent transmits the event line to the end recipient (para [0055], metadata details are passed [claimed transmitting] to the base computer, where, as further disclosed in para [0061], the metadata information is derived from the remote computers [thus, the remote computers, which includes the agent program, will send the metadata information through an associated interface]. Also see para [0014]).

Regarding claim 12, Morris teaches wherein the sensor agent is further operable to: cache the one or more events (para [0035], a local agent [claimed sensor agent] of a remote computer searches a local database stored at the remote computer. Further, as disclosed in para [0039], the local database copies the signature information from a community database for retrieval [thus, the information is cached locally for faster retrieval]); and asynchronously consolidate and normalize the one or more events (para [0093], the agent program on the remote computer coordinates with the ENZO server to update metadata information about which objects have been seen by the community so as not to store duplicated metadata, where, as further disclosed in para [0056], the metadata includes event information. Further, as disclosed in para [0093], this process is initiated when the remote computers and the associated agents receive a data packet [thus, each remote computer will initiate the coordination with the ENZO server dynamically and not in a synchronized operation]).

Regarding claim 13, Morris teaches wherein the at least one event includes information uniquely identifying the object performing the action (para [0056], the event includes information of the object performing the act), information uniquely identifying the action being performed (para [0056], the event includes information of the act being performed), and information uniquely identifying the target upon which the act is being performed (para [0056], the event includes the object or identity of another entity upon which the act is being performed).

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2014/036832

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:

Regarding claim 18, Morris teaches a global perspective information server (para [0073], ENZO central servers that aggregate all of the collected data) including: a processor ([0156]); a communication interface (para [0093] discloses the ENZO server communicates with remote computers [thus, the server will have an associated interface]; data storage (para [0093], ENZO server stores metadata information. Also see para [0073]); and a global perspective module, wherein the global perspective module is operable to: receive the event line from the device (para [0073] discloses aggregate all of the information received from all remote computers [thus, the server will have a global perspective of all metadata information]. Also see para [0074]-[0076] and [0093]); obtain a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object (para [0093] discloses the ENZO server stores all metadata information, where, as further disclosed in para [0056] and [0058], the metadata information may include information of the object performing the act [claimed first object] and the parent object [claimed originating object]), the information including at least one of age (pare [0134], objects having a specific determination, location, popularity, age or any other criteria known by or derived by the database), popularity (para [0134]), a determination as to whether the first object is malware (para [0015], determine whether or not the object is malware), a determination as to whether the originating object is malware (determine whether or not the object is malware. Also see para [0058]); and Internet Protocol (IP) Address or Uniform Resource Locator (URL) information (para [0056], the IP address or URL); assemble a second event line including details associated with the at least one event (para [0093] discloses the ENZO server maintains a master list [claimed second event line] of all metadata information and propagates the list to all remote computers), the details including information uniquely identifying each of the first object (para [0056], metadata information includes events related to objects performing the act), the action of the first object (para [0056] discloses metadata information includes the act being performed), the target (para [0056] discloses metadata information includes the victim), and the originating object (para [0058], metadata information includes parent object); and transmit the assembled second event line utilizing the communication interface to an end recipient (para [0093] discloses the ENZO server maintains a master list [claimed second event line] of all metadata information and propagates the list to all remote computers).

Claims 7, 16 and 19 lack an inventive step under PCT Article 33(3) as being obvious over Morris.

Regarding claim 7, Morris teaches heuristically displaying information identifying the first object performing the action (para [0125] discloses displaying the collected information regarding the monitored objects, where, as further disclosed in para [0061], the collected information in the database include rules and heuristics), information identifying the action being performed (para [0056]), information identifying the target upon which the act is being performed (para [0056]), and the global perspective according to one or more of a location associated with the first object (para [0125] discloses obtaining a collective view of an object including its metadata and behaviors, where, as further disclosed in para [0057], the metadata includes location information. Also see para [0119]); at least one characteristic of an outbound connection associated with the first object (para [0056], a network entity with which an object is communicating); a executable file (para [0111], The data can also be measured against their filenames, and file types (e.g. .exe) [claimed executable file]. Also see para [0058]); an age of the first object (para [0044] discloses monitoring a process [claimed object] for a period of n days [claimed age] to determine whether the process is safe. Also see para [0132]); and connections associated with the first object (para [0056], a network entity with which an object is communicating).
Morris does not teach identifying dropped files and a number of concurrent connections. However, configuring management of data and data connections has been a practice well known in the art and the specifics (identifying dropped files and a number of concurrent connections) would have been a matter of design choice. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate identifying dropped files and a number of concurrent connections in the invention of Morris. The motivation do so would have been to enhance the detection of security attacks by collecting and displaying security related information (Morris, para [0125]).

Regarding claim 16, Morris teaches heuristically displaying information identifying the first object performing the action (para [0125] discloses displaying the collected information regarding the monitored objects, where, as further disclosed in para [0061], the collected information in the database include rules and heuristics), information identifying the action being performed (para [0056]), information identifying the target upon which the act is being performed (para [0056]), and the global perspective according to one or more of a location associated with the first object (para [0125] discloses obtaining a collective view of an object including its metadata and behaviors, where, as further disclosed in para [0057], the metadata includes location information. Also see para [0119]); at least one characteristic of an outbound connection associated with the first object (para [0056], a network entity with which an object is communicating); a executable file (para [0111], The data can also be measured against their filenames, and file types (e.g. .exe) [claimed executable file]. Also see para [0058]); an age of the first object (para [0044] discloses monitoring a process [claimed object] for a period of n days [claimed age] to determine whether the process is safe. Also see para [0132]); and connections associated with the first object (para [0056], a network entity with which an object is communicating).
Morris does not teach identifying dropped files and a number of concurrent connections. However, configuring management of data and data connections has been a practice well known in the art and the specifics (identifying dropped files and a number of concurrent connections) would have been a matter of design choice. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate identifying dropped files and a number of concurrent connections in the invention of Morris. The motivation do so would have been to enhance the detection of security attacks by collecting and displaying security related information (Morris, para [0125]).

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No. PCT/US2014/036832

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:

Regarding claim 19, Morris teaches wherein the end recipient heuristically displays information identifying the first object performing the action (para [0125] discloses displaying the collected information regarding the monitored objects, where, as further disclosed in para [0061], the collected information in the database include rules and heuristics), information identifying the action being performed (para [0056]), information identifying the target upon which the act is being performed (para [0056]), and the global perspective according to one or more of a location associated with the first object (para [0125] discloses obtaining a collective view of an object including its metadata and behaviors, where, as further disclosed in para [0057], the metadata includes location information. Also see para [0119]); at least one characteristic of an outbound connection associated with the first object (para [0056], a network entity with which an object is communicating); a executable file (para [0111], The data can also be measured against their filenames, and file types (e.g. .exe) [claimed executable file]. Also see para [0058]); an age of the first object (para [0044] discloses monitoring a process [claimed object] for a period of n days [claimed age] to determine whether the process is safe. Also see para [0132]); and connections associated with the first object (para [0056], a network entity with which an object is communicating).
Morris does not teach identifying dropped files and a number of concurrent connections. However, configuring management of data and data connections has been a practice well known in the art and the specifics (identifying dropped files and a number of concurrent connections) would have been a matter of design choice. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate identifying dropped files and a number of concurrent connections in the invention of Morris. The motivation do so would have been to enhance the detection of security attacks by collecting and displaying security related information (Morris, para [0125]).

Claims 5-6 and 14-15 lack an inventive step under PCT Article 33(3) as being obvious over Morris in view of Crosby et al (hereinafter Crosby).

Regarding claim 5, Morris teaches determining whether [information] for the at least one event has been cached (para [0035], search a local database stored at the remote computer to search for a signature or key representing that particular process, its related objects and/or the event. Further, as disclosed in para [0039], the local database copies the signature information from a community database for retrieval [thus, the information is cached locally for faster retrieval]); when the [information] for the at least one event has been cached, obtaining [information] for the at least one event based on the cached information (para [0035], If the local signature is present, it will indicate either that the process is considered to be safe or will indicate that that process is considered unsafe [claimed obtaining information based on the stored information]);
and when the [information] for the at least one event has not been cached, obtaining [information] for the at least one event from a community database (para [0039], when a local signature is not found, a community database is searched and used to retrieve the required signature information which is sent to the local computer).
Morris does not teach caching a global perspective. However, Crosby, in analogous art, teaches monitoring security attacks (abstract). Crosby further teaches caching a global perspective (para [0042] discloses a locally storing global beliefs [claimed global perspective] regarding the security state of the system. Also see para [0023] and [0025]). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Crosby to incorporate caching a global perspective in the invention of Morris in order to enhance detection of security attacks (Crosby, para [0042]).

Regarding claim 6, Morris teaches obtaining [information] for the at least one event from a community database (para [0039]).
Morris does not teach determining whether the cached global perspective for the at least one event has expired; and when the global perspective for the at least one event has expired, obtaining a global perspective for the at least one event from a database.
However Crosby, in analogous art, teaches determining whether the cached global perspective for the at least one event has expired (para [0043] discloses whether global beliefs are older than a maximum age value [claimed expired]); and when the global perspective for the at least one event has expired (para [0043], determine whether global belief has exceeded maximum age. Also see para [0023]).
Furthermore, configuring management of data has been a practice well known in the art and the specifics (obtaining a global perspective from a database when the global perspective has expired) would have been a matter of design choice. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Crosby to incorporate retrieval of information from a database when the information has expired in the invention of Morris in order to enhance the detection of new security attacks (Crosby, para [0043]).

Regarding claim 14, Morris teaches determining whether [information] for the at least one event has been cached (para [0035], search a local database stored at the remote computer to search for a signature or key representing that particular process, its related objects and/or the event. Further, as disclosed in para [0039], the local database copies the signature information from a community database for retrieval [thus, the information is cached locally for faster retrieval]);
when the [information] for the at least one event has been cached, obtaining [information] for the at least one event based on the cached information (para [0035], If the local signature is present, it will indicate either that the process is considered to be safe or will indicate that that process is considered unsafe [claimed obtaining information based on the stored information]);
and when the [information] for the at least one event has not been cached, obtaining [information] for the at least one event from a community database (para [0039], when a local signature is not found, a community database is searched and used to retrieve the required signature information which is sent to the local computer).
Morris does not teach caching a global perspective. However, Crosby, in analogous art, teaches monitoring security attacks (abstract). Crosby further teaches caching a global perspective (para [0042] discloses a locally storing global beliefs [claimed global perspective] regarding the security state of the system. Also see para [0023] and [0025]). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Crosby to incorporate caching a global perspective in the invention of Morris in order to enhance detection of security attacks (Crosby, para [0042]).

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2014/036832

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:

Regarding claim 15, Morris teaches obtaining [information] for the at least one event from a community database (para [0039]). Morris does not teach determining whether the cached global perspective for the at least one event has expired; and when the global perspective for the at least one event has expired, obtaining a global perspective for the at least one event from a database. However Crosby, in analogous art, teaches determining whether the cached global perspective for the at least one event has expired (para [0043] discloses whether global beliefs are older than a maximum age value [claimed expired]); and when the global perspective for the at least one event has expired (para [0043], determine whether global belief has exceeded maximum age. Also see para [0023]). Furthermore, configuring management of data has been a practice well known in the art and the specifics (obtaining a global perspective from a database when the global perspective has expired) would have been a matter of design choice. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Crosby to incorporate retrieval of information from a database when the information has expired in the invention of Morris in order to enhance the detection of new security attacks (Crosby, para [0043]).

Claims 20 lack an inventive step under PCT Article 33(3) as being obvious over Morris in view of Fanton et al. (hereinafter Fanton)

Regarding claim 20, Morris teaches a bridge (para [0035], local database) including: a processor (para [0156]); a communication interface (para [0065], the agent program communicates with the local database [thus, the local database will have an associated interface to communicate]; and a cached event store (para [0065], local database holds a local copy [claimed cache]of signatures relating to the objects found on the remote computer), wherein the cached event store is operable to: receive a first request for [information] for the at least one event (para [0035], the local database is searched for signature or key representing a process, its related objects and/or event); receive a second request for a [information] for another event (para [0035] discloses searching a local database to determine whether a monitored object is safe or unsafe [thus, for each new monitored object received at the remote computer, a local database will be searched for associated information regarding the object and its related events]), obtain a first [information] for the at least one event by obtaining information associated with one or more of the first object and the originating object (para [0034]-[0035] discloses searching a local database for metadata information, where, as further disclosed in para [0056] and [0058], the metadata information may include information of the object performing the act [claimed first object] and the parent object [claimed originating object]), the information including at least one of pare [0134], objects having a specific determination, location, popularity, age or any other criteria known by or derived by the database), popularity (para [0134]), a determination as to whether the first object is malware (para [0015], determine whether or not the object is malware), a determination as to whether the originating object is malware (determine whether or not the object is malware. Also see para [0058]); and Internet Protocol (IP) Address or Uniform Resource Locator (URL) information (para [0056], the IP address or URL); obtain a second [information] for the another event (para [0035] discloses searching a local database to determine whether a monitored object is safe or unsafe [thus, for each new monitored object received at the remote computer, a local database will be searched for associated information regarding the object and its related events]); provide the first [information] to the device (para [0035]);
Morris does not teach receive a request for global perspective, a second request for a global perspective from another device, provide the first global perspective to the first device and the second global perspective to the another device. However, Fanton, in analogous art, teaches protecting a computer system from attack (para [0022]). Fanton further teaches receive a request for global perspective, a second request for a global perspective from another device, provide the first global perspective to the first device and the second global perspective to the another device (para [0009] discloses generating and searching [claimed request] a global white list [claimed global perspective] to determine if a program is safe to run, where, as further disclosed in para [0039], the global white list may be maintained in a server for an enterprise network to provide a group wide policy [thus, a first and second end user of the enterprise will search a global white list stored on the server to receive a determination on the end user device to run the program]). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Fanton to incorporate send global perspective information to a first and second device in the invention of Morris in order to enhance the security of enterprise networks (Fanton, para [0039]).

Claims 1-20 meet the criteria set out in PCT Article 33(4), and thus have industrial applicability because the subject matter claimed can be made or used in industry.

Electronic Patent Application Fee Transmittal

Application Number:	15437275
Filing Date:	20-Feb-2017
Title of Invention:	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS
First Named Inventor/Applicant Name:	Joseph Jaroch
Filer:	Andrew T. Pouzeshi/Amy Woodward
Attorney Docket Number:	04584.0021USC1

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
		Total in USD ($)		**180**

Electronic Acknowledgement Receipt

EFS ID:	30133025
Application Number:	15437275
International Application Number:	
Confirmation Number:	4847
Title of Invention:	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS
First Named Inventor/Applicant Name:	Joseph Jaroch
Customer Number:	23552
Filer:	Andrew T. Pouzeshi/Amy Woodward
Filer Authorized By:	Andrew T. Pouzeshi
Attorney Docket Number:	04584.0021USC1
Receipt Date:	21-AUG-2017
Filing Date:	20-FEB-2017
Time Stamp:	13:04:48
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$180
RAM confirmation Number	082117INTEFSW13060900
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	04584_0021USC1_IDS.PDF	1007299 f3e67764e6b7333da7cc492c3bc8ca23579454db	no	5
Warnings:					
Information:					
2	Foreign Reference	WO2006094228A2.PDF	1449365 10e6f574e9a78a04774b9f5ab8ce433e33b81220	no	53
Warnings:					
Information:					
3	Foreign Reference	WO2012110501A1.PDF	521598 592737e71f63de95476bdd3a99cc75124bb3faab	no	84
Warnings:					
Information:					
4	Non Patent Literature	EP_EESR_147918825_2016-11-11_8pgs.PDF	210347 3c103a278f3bd58483ff5022dec148c8d54071e2	no	8
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
5	Non Patent Literature	PCT_IPRP_pctus2014036832_2015-11-03_8pgs.PDF	617124 4f4cb51b8cdba11095a93e7d5a18aa016b675580	no	8
Warnings:					
Information:					
6	Non Patent Literature	PCT_ISR_pctus2014036832_20014-09-29_9pgs.PDF	675109 89cbcab1e68fb60da789dc6abd16145d042f9c81	no	9
Warnings:					

Information:					
7	Non Patent Literature	14270069_amend_2016-03-16_16pgs.PDF	692640 d569658db9d053b7da50ba32652ff86600685629	no	16
Warnings:					
Information:					
8	Non Patent Literature	14270069_amend_2016-08-31_13pgs.PDF	562018 4c61322ae37f2c48e4258665eea16053db37cab9	no	13
Warnings:					
Information:					
9	Non Patent Literature	14270069_NOA_2016-10-05_8pgs.PDF	407158 a071aa3bd9dab9fc0eca1b484e574e6c3053b586	no	8
Warnings:					
Information:					
10	Non Patent Literature	14270069_OA_2015-09-16_12pgs.PDF	502050 f64e4fb16454dadd18f4fd34fd89359cdc2d3f4f	no	12
Warnings:					
Information:					
11	Non Patent Literature	14270069_OA_2016-05-31_11pgs.PDF	464199 e39443a7b111677e8dc76df646d15118065bed95	no	11
Warnings:					
Information:					
12	Fee Worksheet (SB06)	fee-info.pdf	31143 e532d4070ccbab6d0c70963d95d55fcb8cedf0d1	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	7140050	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PATENT
Conf. No. 4847

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Jaroch et al.	Examiner:	Shehni, Ghazal B.
Serial No.:	15/437,275	Group Art Unit:	2436
Filed:	February 20, 2017	Docket No.:	04584.0021USC1
Title:	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS		

AMENDMENT & RESPONSE TO NON-FINAL OFFICE ACTION

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Dear Commissioner:

In response to the Non-Final Office Action mailed April 3, 2017, please amend the above-identified application as follows:

Amendments to the Claims are reflected in the listing of claims that begins on page 2 of this paper.

Remarks/Arguments begin on page 9 of this paper.

Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims:

1. (Currently Amended) A method comprising:

gathering ~~one or more events~~ an event defining an action of a first object acting on a target, wherein the first object is executed on a device;

generating [[a]] contextual state information for ~~at least one of the one or more events~~ the event by correlating the ~~at least one~~ event to an originating object of the first object;~~, the contextual state including an indication of the originating object of the first object and an indication of at least one of a device on which the first object is executed and a user associated with the first object;~~

obtaining a global perspective for the ~~at least one~~ event based on the contextual state information, wherein the global perspective comprises ~~by obtaining~~ information associated with one or more of the first object and the originating object, and wherein the global perspective relates to one or more other events related to the event across a network;~~, the information including at least one of age, popularity, a determination as to whether the first object is malware, a determination as to whether the originating object is malware; and Internet Protocol (IP) Address or Uniform Resource Locator (URL) information;~~

generating ~~assembling~~ an event line ~~including details associated with the at least one~~ comprising information relating to the event, wherein the ~~details including~~ information ~~uniquely identifying each of~~ relates to at least one of the first object, the action of the first object, the target, and the originating object; and

transmitting the generated ~~assembled~~ event line.

2. (Original) The method of claim 1, wherein the information associated with the one or more of the first object and the originating object is obtained from a community database; and

wherein the event line is transmitted to an end recipient.

3. (Currently Amended) The method of claim 1, further comprising:

obtaining an event priority based on one or more of the generated contextual state information and the global perspective ~~for the at least one event~~, wherein the event line further includes the event priority ~~for the at least one event~~.

4. (Currently Amended) The method of claim 1, wherein the ~~at least one~~ event includes information ~~uniquely~~ identifying the object performing the action, information ~~uniquely~~ identifying the action being performed, and information ~~uniquely~~ identifying the target upon which the act is being performed.

5. (Currently Amended) The method of claim 4, further comprising:

determining whether [[a]] the global perspective for the ~~at least one~~ event has been cached;

when the global perspective for the ~~at least one~~ event has been cached, obtaining [[a]] the global perspective for the ~~at least one~~ event based on the cached global perspective; and

when the global perspective for the ~~at least one~~ event has not been cached, obtaining [[a]] the global perspective for the ~~at least one~~ event from a community database.

6. (Currently Amended) The method of claim 5, further comprising:

determining whether the cached global perspective for the ~~at least one~~ event has expired, based on a time-to-live value associated with the cached global perspective; and

when the global perspective for the ~~at least one~~ event has expired, obtaining [[a]] the global perspective for the ~~at least one~~ event from a community database.

7. (Currently Amended) The method of claim 4, further comprising:

heuristically displaying information identifying the first object performing the action, information identifying the action being performed, information identifying the target upon which the act is being performed, and information associated with the global perspective according to one or more of:

a location associated with the first object;

at least one characteristic of an outbound connection associated with the first object;

a dropped executable file;

an age of the first object; and

a number of concurrent connections associated with the first object.

8. (Currently Amended) ~~A computer readable storage medium comprising processor executable instructions operable to perform the~~ The method of claim 1, wherein the global perspective comprises information including at least one of:

an age;

a popularity;

a determination as to whether the first object is malware;

a determination as to whether the originating object is malware;

an Internet Protocol (IP) Address; and

a Uniform Resource Locator (URL).

9. (Currently Amended) A system for providing forensic visibility into a system, comprising:

a device including:

a communication interface;

a processor;

data storage; and

a sensor agent stored on the data storage that is executable by the processor, wherein the sensor agent is operable to:

gather ~~one or more events~~ an event defining an action of a first object acting on a target;

generate [[a]] contextual state information for ~~at least one of the one or more events~~ the event by correlating the ~~at least one~~ event to an originating object of the first object;~~, the contextual state including an indication of the originating object of the first~~

~~object and an indication of at least one of a device on which the first object is executed and a user associated with the first object;~~

obtain a global perspective for the ~~at least one~~ event based on the contextual state information, wherein the global perspective comprises ~~by obtaining~~ information associated with one or more of the first object and the originating object, and wherein the global perspective relates to one or more other events related to the event across a network;~~, the information including at least one of age, popularity, a determination as to whether the first object is malware, a determination as to whether the originating object is malware; and Internet Protocol (IP) Address or Uniform Resource Locator (URL) information;~~

generate ~~assemble~~ an event line ~~including details associated with the at least one~~ comprising information relating to the event, wherein the ~~details including~~ information ~~uniquely identifying each of~~ relates to at least one of the first object, the action of the first object, the target, and the originating object; and

transmit the generated ~~assembled~~ event line utilizing the communication interface.

10. (Currently Amended) The system of claim 9, wherein the event ~~at least one of the one or more events~~ is executed by the processor.

11. (Currently Amended) The system of claim 9, further comprising:

a global perspective information server; and

an end recipient device, wherein the information associated with the one or more of the first object and the originating object is obtained from the global perspective information server and the sensor agent transmits the event line to the end recipient device.

12. (Currently Amended) The system of claim 8, wherein the sensor agent is further operable to:

cache the event and one or more other events; and

asynchronously consolidate and normalize the event and the one or more other events.

13. (Currently Amended) The system of claim 9, wherein the ~~at least one~~ event includes information ~~uniquely~~ identifying the object performing the action, information ~~uniquely~~ identifying the action being performed, and information ~~uniquely~~ identifying the target upon which the act is being performed.

14. (Currently Amended) The system of claim 13, wherein the sensor agent is further operable to:

determine whether [[a]] the global perspective for the ~~at least one~~ event has been cached;

when the global perspective for the ~~at least one~~ event has been cached, obtain [[a]] the global perspective for the ~~at least one~~ event based on the cached global perspective; and

when the global perspective for the ~~at least one~~ event has not been cached, obtain [[a]] the global perspective for the ~~at least one~~ event from a community database.

15. (Currently Amended) The system of claim 14, wherein the sensor agent is further operable to:

determine whether the cached global perspective for the ~~at least one~~ event has expired, based on a time-to-live value associated with the cached global perspective; and

when the global perspective for the ~~at least one~~ event has expired, obtain [[a]] the global perspective for the ~~at least one~~ event from a community database.

16. (Currently Amended) The system of claim 11 [[13]], wherein the end recipient device heuristically displays information identifying the first object performing the action, information identifying the action being performed, information identifying the target upon which the act is being performed, and information associated with the global perspective according to one or more of:

a location associated with the first object;

at least one characteristic of an outbound connection associated with the first object;

a dropped executable file;

an age of the first object; and

a number of concurrent connections associated with the first object.

17. (Currently Amended) A system for providing forensic visibility into a system, comprising:

a device including:

a communication interface;

a processor;

data storage; and

a sensor agent stored on the data storage that is executable by the processor, wherein the sensor agent is operable to:

gather ~~one or more events~~ an event defining an action of a first object acting on a target;

determine a global perspective for the event based on ~~generate a~~ contextual state information for the event, wherein the global perspective relates to one or more other events related to the event across a network, and wherein the contextual state comprises ~~for at least one of the one or more events by correlating the at least one event to an originating object, the contextual state including~~ an indication of [[the]] an originating object of the first object and an indication of at least one of a device on which the first object is executed and a user associated with the first object;

generate ~~assemble~~ an event line ~~including details associated with the at least one~~ comprising information relating to the event, wherein the ~~details including~~ information ~~uniquely identifying each of~~ relates to at least one of the first object, the action of the first object, the target, and the originating object; and

transmit the generated ~~assembled~~ event line utilizing the communication interface.

18. (Currently Amended) The system of claim 17, further comprising a global perspective information server including:

a processor;

a communication interface;

data storage; and

a global perspective module, wherein the global perspective module is operable to:

receive the event line from the device;

~~obtain a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object, the information including at least one of age, popularity, a determination as to whether the first object is malware, a determination as to whether the originating object is malware; and Internet Protocol (IP) Address or Uniform Resource Locator (URL) information;~~

assemble a second event line including details associated with the ~~at least one~~ event, wherein the second event line comprises ~~the details including~~ information ~~uniquely~~ identifying each of the first object, the action of the first object, the target, and the originating object; and

transmit the ~~assembled~~ second event line utilizing the communication interface to an end recipient.

19. (Currently Amended) The system of claim 18, wherein the end recipient heuristically displays information identifying the first object performing the action, information identifying the action being performed, information identifying the target upon which the act is being performed, and information associated with the global perspective according to one or more of:

a location associated with the first object;

at least one characteristic of an outbound connection associated with the first object;

a dropped executable file;

an age of the first object; and

a number of concurrent connections associated with the first object.

20. (Currently Amended) The system of claim 17, further comprising a bridge including:

a processor;

a communication interface; and

a cached event store, wherein the cached event store is operable to:

receive a first request for a global perspective for the ~~at least one~~ event;

receive a second request for a global perspective for another event, the second request originating from another device;

obtain a first global perspective for the ~~at least one~~ event by obtaining information associated with one or more of the first object and the originating object~~, the information including at least one of age, popularity, a determination as to whether the first object is malware, a determination as to whether the originating object is malware; and Internet Protocol (IP) Address or Uniform Resource Locator (URL) information~~;

obtain a second global perspective for the another event;

provide the first global perspective to the device; and

provide the second global perspective to the another device.

REMARKS/ARGUMENTS

This Amendment and the following remarks are intended to fully respond to the non-final Office Action dated April 3, 2017, hereinafter "Office Action." In that Office Action, claims 1-20 were examined and all claims were rejected. Claim 8 was rejected under 35 U.S.C. § 101 for allegedly being directed to non-statutory subject matter. Claims 5, 11, and 14 were rejected under 35 U.S.C. § 112, second paragraph, for allegedly failing to particularly point out and distinctly claim the subject matter that Applicants regard as their invention. Claim 8 was rejected under 35 U.S.C. § 112, fourth paragraph, for allegedly being of improper dependent form for failing to further limit the subject matter of the claim upon which it depends, or for failing to include all the limitations of the claim upon which it depends. Claims 1-20 were rejected under 35 U.S.C. § 103 as being unpatentable over Kumar et al. (U.S. Publ. No. 2013/0298244; hereinafter "Kumar") in view of Capalik (U.S. Publ. No. 2008/0016570; hereinafter "Capalik").

Reconsideration of these rejections, as they might apply to the original and amended claims in view of these remarks, is respectfully requested. In this Amendment, claims 1 and 3-20 have been amended, no claims have been canceled, and no claims have been added. Therefore, claims 1-20 remain present for examination.

Nonstatutory Double Patenting

Claims 1-20 are rejected on the ground of nonstatutory double patenting as being unpatentable over claims 1-19 of U.S. Patent No. 9,578,045. Without acquiescing to the propriety of the rejection and solely for the purpose of advancing prosecution, Applicants will file a terminal disclaimer, if necessary, when otherwise allowable subject matter has been indicated.

Claim Rejections Under 35 U.S.C. § 101

Claim 8 was rejected under 35 U.S.C. § 101 for allegedly being directed to non-statutory subject matter. More specifically, the Office Action alleges that "claim 8 is not described in the specification as including a tangible medium in a manner which enables it to act as a computer component to realize the computer program's functionality." (Office Action, pg. 4.)

Claim 8 has been amended to recite "The method of claim 1, wherein the global perspective comprises information including at least one of: an age; a popularity; a determination as to whether the first object is malware; a determination as to whether the originating object is malware; an Internet Protocol (IP) Address; and a Uniform Resource Locator (URL)." As such, Applicants respectfully submit that claim 8 recites statutory subject matter and request that the Examiner withdraw the rejection and allow claim 8 at the Examiner's earliest convenience.

Claim Rejections Under 35 U.S.C. § 112

Claims 5 and 14

Claims 5 and 14 were rejected under 35 U.S.C. § 112, second paragraph, for allegedly failing to particularly point out and distinctly claim the subject matter that Applicants regard as their invention. As such, claims 5 and 14 have been amended to recite "the global perspective." In light of this amendment, Applicants respectfully request that the Examiner withdraw the rejection and allow claims 5 and 14 at the Examiner's earliest convenience.

Claim 11

Claim 11 was rejected under 35 U.S.C. § 112, second paragraph, for allegedly failing to particularly point out and distinctly claim the subject matter that Applicants regard as their invention. Accordingly, claim 11 has been amended to recite "the end recipient device." In light of this amendment, Applicants respectfully request that the Examiner withdraw the rejection and allow claim 11 at the Examiner's earliest convenience.

Claim 8

Claim 8 was rejected under 35 U.S.C. § 112, fourth paragraph, for allegedly being of improper dependent form for failing to further limit the subject matter of the claim upon which it depends, or for failing to include all the limitations of the claim upon which it depends. Applicants respectfully submit that claim 8 has been amended to be in proper dependent form. As such, Applicants request that the Examiner withdraw the rejection and allow claim 8 at the Examiner's earliest convenience.

Claim Rejections Under 35 U.S.C. § 103

Claims 1-20 were rejected under 35 U.S.C. § 103 as being unpatentable over Kumar in view of Capalik. Applicants respectfully traverse the § 103 rejection because the Office Action has not established a *prima facie* case of obviousness. To establish a *prima facie* case of obviousness under 35 U.S.C. § 103, the references must teach or suggest all of the claimed limitations to one of ordinary skill in the art at the time the invention was made. M.P.E.P §§ 2142, 2143.03; *In re Royka*, 490 F.2d 981, 985 (C.C.P.A. 1974); *In re Wilson*, 424 F.2d 1382, 1385 (C.C.P.A. 1970). Further, under *KSR Int'l Co. v. Teleflex, Inc.*, there "must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." 127 S. Ct. 1727, 1741 (2007). Applicants traverse the rejection because the references fail to teach or suggest all of the recited limitations of the claims.

In nonlimiting, nonexclusive examples, aspects of the present application relate to providing forensic visibility into systems and networks. In an example, a sensor agent may receive an event defining an action of a first object acting on a target. Contextual state information may be generated for the event by correlating the event to an originating object, such that an audit trail for each individual event may be created. In some examples, a global perspective may be obtained based on the contextual state information, which may comprise information associated with the first object and/or the originating object. In another example, the global perspective may relate to one or more other events related to the event across a network. An event line comprising event information may be generated and communicated to a recipient.

By contrast, Kumar relates to methods for threat identification and remediation. Kumar teaches a security orchestration service that generates runtime operational integrity profiles representing level of threat or contextual trustworthiness of subjects and applications within a target platform. (*See* Kumar, Abstract.) A system event correlator is used to map alerts within the target platform to a specific cell in a risk correlation matrix, which "illustrates that *for each device* . . . , a different set of alerts may trigger different system warning that map to a common system warning class." (Kumar, paras. [0110] and [0131], emphasis added.) Ultimately, an integrity profile for a system is generated based on entries in the appropriate risk correlation matrix row (e.g., for the right machine identifier). (*See* Kumar, para. [0131].)

Turning now to the claims, Kumar fails to teach or suggest at least "obtaining a global perspective for the event based on the contextual state information, wherein the global perspective comprises information associated with one or more of the first object and the originating object, and wherein the global perspective relates to one or more other events related to the event across a network," as recited by independent claim 1. The Office Action alleges that Kumar teaches "risk correlation matrix illustrates that for each device uniquely identified by a machine identifier . . . by mapping alerts to a behavior model threats may be classified." (Office Action, pg. 6.)

However, as discussed above, Kumar merely teaches mapping threats to a cell within a risk correlation matrix and using the matrix to determine a state for a device within a target platform. Indeed, Kumar discloses a matrix that comprises information on a device-by-device basis and is associated with a machine or application identifier. (*See* Kumar, Figure 7C and paras. [0130]-[0131].) It is illogical to conclude that such a simplistic mapping of alerts to a specific device is analogous to the claimed "global perspective" that is "based on the contextual state information" and "relates to one or more other events related to the event across a network." Rather, Kumar is focused on the integrity of a single application running on a single device. There is simply no teaching of events relating to application integrity for other devices on a network. Therefore, Kumar cannot possibly teach or suggest a "global perspective" that "relates to one or more other events related to the event across a network." As such, Applicants respectfully request that the Examiner withdraw the rejection of claim 1 at the Examiner's earliest convenience.

The Office Action cites to Capalik to remedy the deficiencies of Kumar. However, Capalik is similarly unavailing. Indeed, the Office Action does not allege that Capalik teaches the above claim elements but rather cites Capalik with respect to other claim elements. Capalik relates to capturing unauthorized intrusions into a computer using a hypervisor and generating a signature to identify and prevent similar attacks in the future. (*See* Capalik, Abstract.) However, similar to Kumar, Capalik fails to teach or suggest at least "obtaining a global perspective for the event based on the contextual state information, wherein the global perspective comprises information associated with one or more of the first object and the originating object, and

wherein the global perspective relates to one or more other events related to the event across a network," as recited by independent claim 1. Thus, independent claim 1 is allowable over the cited references.

The other independent claims recite similar limitations as claim 1 and are thus also allowable for at least similar reasons. For example, claim 9 recites, *inter alia*, "obtain a global perspective for the event based on the contextual state information, wherein the global perspective comprises information associated with one or more of the first object and the originating object, and wherein the global perspective relates to one or more other events related to the event across a network." Thus, claim 9 is allowable over the cited references for at least similar reasons as were discussed above with respect to claim 1.

For at least similar reasons, independent claim 17 is allowable over the cited references. Claim 17 recites, *inter alia*, "determine a global perspective for the event based on contextual state information for the event, wherein the global perspective relates to one or more other events related to the event across a network, and wherein the contextual state comprises an indication of an originating object of the first object and an indication of at least one of a device on which the first object is executed and a user associated with the first object." Thus, claim 17 is allowable over the cited references for at least similar reasons as were discussed above with respect to claim 1.

For at least the foregoing reasons, independent claims 1, 9, and 17 are allowable over the cited references. All other claims, *i.e.*, claims 2-8, 10-16, and 18-20, depend from one of allowable claims 1, 9, or 17 and, thus, are also allowable. As such, Applicants respectfully request that the Examiner issue a Notice of Allowance for claims 1-20 at the Examiner's earliest convenience.

CONCLUSION

This Amendment fully responds to the Office Action mailed on April 3, 2017. Still, that Office Action may contain arguments and rejections that are not directly addressed by this Amendment due to the fact that they are rendered moot in light of the preceding arguments in favor of patentability. Hence, failure of this Amendment to directly address an argument raised in the Office Action should not be taken as an indication that the Applicants believe the argument has merit. Furthermore, the claims of the present application may include other elements, not discussed in this Amendment, which are not shown, taught, or otherwise suggested by the references of record. Accordingly, the preceding arguments in favor of patentability are advanced without prejudice to other bases of patentability.

This Amendment is filed concurrently with a Petition for Extension of Time. It is believed that no further fees are due with this Response. However, the Commissioner is hereby authorized to charge any deficiencies or credit any overpayment with respect to this patent application to deposit account number 13-2725.

In light of the above remarks and amendments, it is believed that the application is now in condition for allowance and such action is respectfully requested. Should any additional issues need to be resolved, the Examiner is requested to telephone the undersigned to attempt to resolve those issues.

Respectfully submitted,

Dated: __September 5, 2017__

/Ethan W. Bell/

Ethan W. Bell, Reg. No. 75,549
Merchant & Gould P.C.
P.O. Box 2903
Minneapolis, MN 55402-0903
(303) 357-1211

23552
PATENT TRADEMARK OFFICE

PTO/AIA/22 (03-13)
Approved for use through 7/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)

Docket Number (Optional): 04584.0021USC1

Application Number	Filed
15/437,275	02-20-2017

For: METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS

Art Unit	Examiner
2436	SHEHNI, GHAZAL B

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above-identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

	Fee	Small Entity Fee	Micro Entity Fee	
☐ One month (37 CFR 1.17(a)(1))	$200	$100	$50	$
☑ Two months (37 CFR 1.17(a)(2))	$600	$300	$150	$ 600.00
☐ Three months (37 CFR 1.17(a)(3))	$1,400	$700	$350	$
☐ Four months (37 CFR 1.17(a)(4))	$2,200	$1,100	$550	$
☐ Five months (37 CFR 1.17(a)(5))	$3,000	$1,500	$750	$

☐ Applicant asserts small entity status. See 37 CFR 1.27.

☐ Applicant certifies micro entity status. See 37 CFR 1.29.
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

☐ A check in the amount of the fee is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☑ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 132725.

☑ Payment made via EFS-Web.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant.

☑ attorney or agent of record. Registration number 75,549.

☐ attorney or agent acting under 37 CFR 1.34. Registration number _____.

/Ethan W. Bell/	2017-09-05
Signature	Date
Ethan W. Bell	303-357-1211
Typed or printed name	Telephone Number

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☑ * Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.136(a). The information is required to obtain or retain a benefit by the public, which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 6 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop PCT, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal

Application Number:	15437275
Filing Date:	20-Feb-2017
Title of Invention:	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS
First Named Inventor/Applicant Name:	Joseph Jaroch
Filer:	Ethan Wendel Bell/Amy Woodward
Attorney Docket Number:	04584.0021USC1

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 2 months with $0 paid	1252	1	600	600
Miscellaneous:				
			Total in USD ($)	**600**

Electronic Acknowledgement Receipt

EFS ID:	30273836
Application Number:	15437275
International Application Number:	
Confirmation Number:	4847
Title of Invention:	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS
First Named Inventor/Applicant Name:	Joseph Jaroch
Customer Number:	23552
Filer:	Ethan Wendel Bell/Amy Woodward
Filer Authorized By:	Ethan Wendel Bell
Attorney Docket Number:	04584.0021USC1
Receipt Date:	05-SEP-2017
Filing Date:	20-FEB-2017
Time Stamp:	17:43:12
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$600
RAM confirmation Number	090617INTEFSW17435100
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		04584_0021USC1_RespNFOA.PDF	153623 0d3ad57efc4928eb75977ea5ed025868785bf13e	yes	15
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Amendment/Req. Reconsideration-After Non-Final Reject		1	1	
	Claims		2	9	
	Applicant Arguments/Remarks Made in an Amendment		10	15	
Warnings:					
Information:					
2	Extension of Time	04584_0021USC1_EOT_RespNFOA.PDF	280519 8b7631484e82b8213ec6b6f6d7084594d447c46c	no	2
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	31180 1ff617fc830eecc518ba0e200c337f26c27ece61	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	465322		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 15/437,275	Filing Date 02/20/2017	☐ To be Mailed

ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT **09/05/2017**

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 20	Minus	** 20	= 0	X $80 =	0
Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X $420 =	0
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	0

AMENDMENT

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
DIANE FLOYD

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/437,275	02/20/2017	Joseph Jaroch	04584.0021USC1	4847

23552 7590 11/22/2017

MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

EXAMINER
SHEHNI, GHAZAL B

ART UNIT	PAPER NUMBER
2436	

NOTIFICATION DATE	DELIVERY MODE
11/22/2017	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

USPTO23552@merchantgould.com

Office Action Summary	Application No. 15/437,275	Applicant(s) JAROCH ET AL.	
	Examiner GHAZAL SHEHNI	Art Unit 2436	AIA (First Inventor to File) Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09/05/2017*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) *1-20* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-20* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date *08/21/2017*.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

1. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

DETAILED ACTION

The following is a final office action in response to communications received 09/05/2017. Claims 1, 3-20 have been amended. Therefore, claims 1-20 are pending and addressed below.

Response to Amendment

Applicant's amendments to the claims are sufficient to overcome the 35 USC 101 rejections and the 35 USC 112, second paragraph, rejections set forth in the previous office action. Examiner maintains the Double Patenting rejections set forth in the previous office action.

Response to Arguments

Applicant's arguments filed 09/05/2017 have been fully considered and they are persuasive.

Double Patenting Rejections

2. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

3. A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

4. Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

5. Claims 1-20 are rejected on the ground of nonstatutory double patenting as being unpatentable over claims 1-19 of U.S. Patent No. 9578045. Although the claims at issue are not identical, they are not patentably distinct from each other because Claims of patent application contain every element of claims above instant application or vice versa, and as such they anticipate or anticipated by Instant Application.

Conclusion

6. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to GHAZAL SHEHNI whose telephone number is (571)270-7479. The examiner can normally be reached on Monday-Thursday.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gelagay Shewaye can be reached on (571)272-4219. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/GHAZAL SHEHNI/

Primary Examiner, Art Unit 2436

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (03-15)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	15437275
Filing Date	2017-02-20
First Named Inventor	Joseph Jaroch
Art Unit	2436
Examiner Name	SHEHNI, GHAZAL B
Attorney Docket Number	04584.0021USC1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/G.B.S/	1	7895649		2011-02-22	Brook et al.	
/G.B.S/	2	9578045		2017-02-21	Jaroch et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/G.B.S/	1	20060095963		2006-05-04	Crosby et al.	
/G.B.S/	2	20080244694		2008-10-02	Neystadt et al.	
/G.B.S/	3	20090300769		2009-12-03	Srinivasa et al.	
/G.B.S/	4	20120072725		2012-03-22	Fanton et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15437275
	Filing Date	2017-02-20
	First Named Inventor	Joseph Jaroch
	Art Unit	2436
	Examiner Name	SHEHNI, GHAZAL B
	Attorney Docket Number	04584.0021USC1

/G.B.S/	5	20120260340		2012-10-11	Morris et al.			

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
/G.B.S/	1	2006094228	WO		2006-09-08	Shull et al.		
/G.B.S/	2	2012110501	WO		2012-08-23	Morris et al.		

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
/G.B.S/	1	European Extended Search Report in Application 14791882.5, mailed 2016-11-11, 8 pages.	
/G.B.S/	2	PCT International Preliminary Report on Patentability in PCT/US2014/036832, mailed 2015-11-03, 8 pages.	
/G.B.S/	3	PCT International Search Report in PCT/US2014/036832, mailed 2014-09-29, 9 pages.	
/G.B.S/	4	US Patent Application 14/270,069, Amendment and Response filed 2016-03-16, 16 pages.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15437275
	Filing Date	2017-02-20
	First Named Inventor	Joseph Jaroch
	Art Unit	2436
	Examiner Name	SHEHNI, GHAZAL B
	Attorney Docket Number	04584.0021USC1

/G.B.S/	5	US Patent Application 14/270,069, Amendment and Response filed 2016-08-31, 13 pages.	
/G.B.S/	6	US Patent Application 14/270,069, Notice of Allowance mailed 2016-10-05, 8 pages.	
/G.B.S/	7	US Patent Application 14/270,069, Office Action mailed 2015-09-16, 12 pages.	
/G.B.S/	8	US Patent Application 14/270,069, Office Action mailed 2016-05-31, 11 pages.	

If you wish to add additional non-patent literature document citation information please click the Add button [Add]

EXAMINER SIGNATURE

Examiner Signature	/GHAZAL B SHEHNI/	Date Considered	11/17/2017

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	15437275
Filing Date	2017-02-20
First Named Inventor	Joseph Jaroch
Art Unit	2436
Examiner Name	SHEHNI, GHAZAL B
Attorney Docket Number	04584.0021USC1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Andrew T. Pouzeshi/	Date (YYYY-MM-DD)	2017-08-21
Name/Print	Andrew T. Pouzeshi	Registration Number	67672

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /G.B.S/

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L9	1	("20120260340").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2017/11/17 15:06

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L8	3	(analys$4 or captur$3 or record$3) near7 ((id or identification or identifier) with ((event or computer or file or program or web$page or web$site or site) with network))with security with (sniffer or malicious or virus or trojan or spy$ware)	US-PGPUB; USPAT	ADJ	ON	2017/11/17 14:57
L7	0	(analys$4 or captur$3 or record$3) near7 (trigger$3 with ((event or computer or file or program or web$page or web$site or site) with network))with security with (sniffer or malicious or virus or trojan or spy$ware)	US-PGPUB; USPAT	ADJ	ON	2017/11/17 14:55
L6	175	(defin$ or analyz$3) with ((behavior or event or computer file or file or program or web$page or web$site) with (network)) with security with (sniffer or malicious or virus or trojan or spy$ware)	US-PGPUB; USPAT	ADJ	ON	2017/11/17 14:48
L5	69	(analys$4 or captur$3 or record$3) near7 ((event or computer or file or program or web$page or web$site or site) with network) with security with (sniffer or malicious or virus or trojan or spy$ware)	US-PGPUB; USPAT	ADJ	ON	2017/11/17 14:29
L4	6	sniffers with (analysis with forensic)	US-PGPUB; USPAT	ADJ	ON	2017/11/17 14:27
L2	134	(analysis with forensic) with (network with event)	US-PGPUB; USPAT	ADJ	ON	2017/11/17 14:27
L1	10843	(analysis with forensic)	US-PGPUB; USPAT	ADJ	ON	2017/11/17 14:26

11/ 17/ 2017 3:17:51 PM
C:\ Users\ gshehni\ Documents\ EAST\ Workspaces\ 15437275.wsp

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15437275	JAROCH ET AL.
	Examiner	**Art Unit**
	GHAZAL SHEHNI	2436

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	03/28/2017	11/17/2017							
	1	✓	✓							
	2	✓	✓							
	3	✓	✓							
	4	✓	✓							
	5	✓	✓							
	6	✓	✓							
	7	✓	✓							
	8	✓	✓							
	9	✓	✓							
	10	✓	✓							
	11	✓	✓							
	12	✓	✓							
	13	✓	✓							
	14	✓	✓							
	15	✓	✓							
	16	✓	✓							
	17	✓	✓							
	18	✓	✓							
	19	✓	✓							
	20	✓	✓							

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15437275	JAROCH ET AL.
	Examiner	Art Unit
	GHAZAL SHEHNI	2436

CPC- SEARCHED		
Symbol	Date	Examiner
H04L63/1416 OR H04L63/20 OR H04L63/1425 OR H04L63/1441 OR H04L63/1408 OR H04L63/1433 OR H04L63/145 OR H04L63/14 OR H04L9/3271 OR H04L12/2602	3/28/2017	GS

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor search (see search history printout)	3/28/2017	GS
East (see search history printout)	3/28/2017	GS
CPC with text search	3/28/2017	GS
East (see search history printout)	11/17/2017	GS

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

	/GHAZAL SHEHNI/ Primary Examiner, Art Unit 2436

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Joseph Jaroch et al.	Examiner:	Shehni, Ghazal B.
Serial No.:	15/437,275	Group Art Unit:	2436
Filed:	February 20, 2017	Docket No.:	04584.0021USC1
Title:	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS		

RESPONSE TO FINAL OFFICE ACTION

Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Dear Commissioner:

In response to the Final Office Action mailed November 22, 2017, please amend the above-identified application as follows:

Remarks begin on page 2 of this paper.

REMARKS/ARGUMENTS

This Amendment and the following remarks are intended to fully respond to the final Office Action dated November 22, 2017, hereinafter "Office Action." In that Office Action, claims 1-20 were examined and all claims were rejected.

Double Patenting Rejection

Claims 1-20 were rejected on the ground of nonstatutory double patenting over U.S. Patent No. 9,578,045. Applicants file a terminal disclaimer over Patent No. 9,578,045. Accordingly, the rejection is obviated and Applicants respectfully request withdrawal of the rejection and allowance of claims 1-20 at the Examiner's earliest convenience.

CONCLUSION

This Amendment fully responds to the Office Action mailed on November 22, 2017. Still, that Office Action may contain arguments and rejections that are not directly addressed by this Amendment due to the fact that they are rendered moot in light of the preceding arguments in favor of patentability. Hence, the failure, if any, of this Amendment and Response to directly address an argument and/or comment raised in the Office Action should not be taken as an indication that the Applicants believe the argument and/or comment has merit. Additionally, the failure, if any, to address statements and/or comments made in the Office Action does not mean that the Applicants acquiesce to such statements and/or comments. Furthermore, the claims of the present application may include other elements, not discussed in this Amendment and Response, which are not shown, taught, or otherwise suggested by the art of record. Accordingly, the preceding arguments in favor of patentability are advanced without prejudice to other bases of patentability.

It is believed that no further fees are due with this Response. However, the Commissioner is hereby authorized to charge any deficiencies or credit any overpayment with respect to this patent application to deposit account number 13-2725.

In light of the above remarks and amendments, it is believed that the application is now in condition for allowance and such action is respectfully requested. Should any additional issues need to be resolved, the Examiner is requested to telephone the undersigned to attempt to resolve those issues.

Respectfully submitted,

Date: February 22, 2018

/Ethan W. Bell/

Ethan W. Bell, Reg. No. 75,549
Merchant & Gould P.C.
P.O. Box 2903
Minneapolis, MN 55402-0903
(303) 357-1211

27488
PATENT TRADEMARK OFFICE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor:	Joseph Jaroch et al.	Examiner:	Shehni, Ghazal B.
Serial No.:	15/437,275	Group Art Unit:	2436
Filed:	February 20, 2017	Docket No.:	04584.0021USC1
Title:	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS		

Filed via EFS-Web

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT (37 C.F.R. § 1.97(d))

Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Attention: Commissioner for Patents

With regard to the above-identified application, the items of information listed on the enclosed Form PTO/SB/08a are brought to the attention of the Examiner.

This statement should be considered because it is submitted after the mailing date of a final action under 37 C.F.R. § 1.113 or after the mailing date of the Notice of Allowance under 37 C.F.R. § 1.311 or after any other action that closes prosecution on the application, but before the payment of the issue fee. Payment is being made via credit card in the amount of $240.00 under 37 C.F.R. § 1.17(p) for consideration of the items listed on the enclosed Form PTO/SB/08a. This statement is submitted as certified below under 37 C.F.R. § 1.97(e)(1) or (2) by the undersigned.

Certification Under 37 C.F.R. § 1.97(e)(1)

In accordance with 37 C.F.R. § 1.97(c) or § 1.97(d), the undersigned hereby certifies that each item of information listed on the enclosed Form PTO/SB/08a was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to filing this statement.

In accordance with 37 C.F.R. § 1.98(a)(2), a copy of each foreign patent and/or a copy of each publication, other than U.S. patents and U.S. patent application publications, listed on the accompanying Form PTO/SB/08a is enclosed.

No representation is made that a reference is "prior art" within the meaning of 35 U.S.C. §§ 102 and 103 and Applicants reserve the right, pursuant to 37 C.F.R. § 1.131 or otherwise, to establish that the reference(s) are not "prior art."

Consideration of the items listed is respectfully requested. Pursuant to the provisions of M.P.E.P. 609, it is requested that the Examiner return a copy of the attached Form PTO/SB/08a, marked as being considered and initialed by the Examiner, to the undersigned with the next official communication.

Please charge any additional fees or credit any overpayment to Deposit Account No. 13-2725.

Respectfully submitted,

Date: February 22, 2018

/Ethan W. Bell/

Ethan W. Bell, Reg. No. 75,549
Merchant & Gould P.C.
P.O. Box 2903
Minneapolis, MN 55402-0903
(303) 357-1211

23552
PATENT TRADEMARK OFFICE

PTO/SB/08a (03-15)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	15437275
Filing Date	2017-02-20
First Named Inventor	Joseph JAROCH
Art Unit	2436
Examiner Name	Shehni, Ghazal B.
Attorney Docket Number	04584.0021USC1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15437275
	Filing Date	2017-02-20
	First Named Inventor	Joseph JAROCH
	Art Unit	2436
	Examiner Name	Shehni, Ghazal B.
	Attorney Docket Number	04584.0021USC1

	1	European Office Action in Application 14791882.5, mailed 2017-12-08, 6 pages.

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15437275
	Filing Date	2017-02-20
	First Named Inventor	Joseph JAROCH
	Art Unit	2436
	Examiner Name	Shehni, Ghazal B.
	Attorney Docket Number	04584.0021USC1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

X That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

X See attached certification statement.

X The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Ethan W. Bell/	Date (YYYY-MM-DD)	2018-02-22
Name/Print	Ethan W. Bell	Registration Number	75,549

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal

Application Number:	15437275
Filing Date:	20-Feb-2017
Title of Invention:	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS
First Named Inventor/Applicant Name:	Joseph Jaroch
Filer:	Ethan Wendel Bell/Julie Borrego
Attorney Docket Number:	04584.0021USC1

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	240	240
		Total in USD ($)		**240**

Electronic Acknowledgement Receipt

EFS ID:	31857821
Application Number:	15437275
International Application Number:	
Confirmation Number:	4847
Title of Invention:	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS
First Named Inventor/Applicant Name:	Joseph Jaroch
Customer Number:	23552
Filer:	Ethan Wendel Bell/Julie Borrego
Filer Authorized By:	Ethan Wendel Bell
Attorney Docket Number:	04584.0021USC1
Receipt Date:	22-FEB-2018
Filing Date:	20-FEB-2017
Time Stamp:	12:32:21
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$240
RAM confirmation Number	022218INTEFSW12331800
Deposit Account	132725
Authorized User	Julie Borrego

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

37 CFR 1.16 (National application filing, search, and examination fees)

37 CFR 1.17 (Patent application and reexamination processing fees)

37 CFR 1.19 (Document supply fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		2018_02_22_RESP_FOA_04584_0021USC1.pdf	87603 16d75c1aa8a1692e44ff246e202d3a3d39afe6ca	yes	3

Multipart Description/PDF files in .zip description

Document Description	Start	End
Response After Final Action	1	1
Applicant Arguments/Remarks Made in an Amendment	2	3

Warnings:

Information:

2	Transmittal Letter	2018_02_22_SIDS_TRANS_LTR_04584_0021USC1.pdf	86178 b016b6627b7cbbe5d7956d7a966f42582025b7b9	no	2

Warnings:

Information:

3	Information Disclosure Statement (IDS) Form (SB08)	2018_02_22_SIDS_1449_04584_0021USC1.pdf	1006857 ba97157938abba44dd7a4d87029ef71fc7972f92	no	4

Warnings:

Information:

A U.S. Patent Number Citation or a U.S. Publication Number Citation is required in the Information Disclosure Statement (IDS) form for autoloading of data into USPTO systems. You may remove the form to add the required data in order to correct the Informational Message if you are citing U.S. References. If you chose not to include U.S. References, the image of the form will be processed and be made available within the Image File Wrapper (IFW) system. However, no data will be extracted from this form. Any additional data such as Foreign Patent Documents or Non Patent Literature will be manually reviewed and keyed into USPTO systems.

4	Non Patent Literature	EP_OA_147918825_2017-12-08.PDF	158189 bd7fe579c116376e3106dc46dd214d8673f691c9	no	6

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

5	Fee Worksheet (SB06)	fee-info.pdf	30963 1bca3d0dd40b56e2d08b0136c3df94b740af8a28	no	2

Warnings:	
Information:	
Total Files Size (in bytes):	1369790

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Doc Code: DIST.E.FILE Document Description: Electronic Terminal Disclaimer - Filed	PTO/SB/26 U.S. Patent and Trademark Office Department of Commerce

Electronic Petition Request	**TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT**
Application Number	15437275
Filing Date	20-Feb-2017
First Named Inventor	Joseph Jaroch
Attorney Docket Number	04584.0021USC1
Title of Invention	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS

☒ Filing of terminal disclaimer does not obviate requirement for response under 37 CFR 1.111 to outstanding Office Action

☒ This electronic Terminal Disclaimer is not being used for a Joint Research Agreement.

Owner	Percent Interest
Webroot Inc.	100%

The owner(s) with percent interest listed above in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of prior patent number(s)

9578045

as the term of said prior patent is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the prior patent are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term of the prior patent, "as the term of said prior patent is presently shortened by any terminal disclaimer," in the event that said prior patent later:
- expires for failure to pay a maintenance fee;
- is held unenforceable;
- is found invalid by a court of competent jurisdiction;
- is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
- has all claims canceled by a reexamination certificate;
- is reissued; or
- is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

◉ Terminal disclaimer fee under 37 CFR 1.20(d) is included with Electronic Terminal Disclaimer request.

○ I certify, in accordance with 37 CFR 1.4(d)(4), that the terminal disclaimer fee under 37 CFR 1.20(d) required for this terminal disclaimer has already been paid in the above-identified application.	

Applicant claims the following fee status:

○ Small Entity

○ Micro Entity

◉ Regular Undiscounted

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

THIS PORTION MUST BE COMPLETED BY THE SIGNATORY OR SIGNATORIES

I certify, in accordance with 37 CFR 1.4(d)(4) that I am:

◉ An attorney or agent registered to practice before the Patent and Trademark Office who is of record in this application

Registration Number 75549

○ A sole inventor

○ A joint inventor; I certify that I am authorized to sign this submission on behalf of all of the inventors as evidenced by the power of attorney in the application

○ A joint inventor; all of whom are signing this request

Signature	/Ethan W. Bell/
Name	Ethan W. Bell

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).
Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

Electronic Patent Application Fee Transmittal

Application Number:	15437275
Filing Date:	20-Feb-2017
Title of Invention:	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS
First Named Inventor/Applicant Name:	Joseph Jaroch
Filer:	Ethan Wendel Bell/Julie Borrego
Attorney Docket Number:	04584.0021USC1

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
STATUTORY OR TERMINAL DISCLAIMER	1814	1	160	160
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**160**

Doc Code: DISQ.E.FILE
Document Description: Electronic Terminal Disclaimer – Approved

Application No.: 15437275

Filing Date: 20-Feb-2017

Applicant/Patent under Reexamination: Jaroch

Electronic Terminal Disclaimer filed on February 22, 2018

☒ APPROVED

This patent is subject to a terminal disclaimer

☐ DISAPPROVED

Approved/Disapproved by: Electronic Terminal Disclaimer automatically approved by EFS-Web

U.S. Patent and Trademark Office

Electronic Acknowledgement Receipt

EFS ID:	31858978
Application Number:	15437275
International Application Number:	
Confirmation Number:	4847
Title of Invention:	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS
First Named Inventor/Applicant Name:	Joseph Jaroch
Customer Number:	23552
Filer:	Ethan Wendel Bell/Julie Borrego
Filer Authorized By:	Ethan Wendel Bell
Attorney Docket Number:	04584.0021USC1
Receipt Date:	22-FEB-2018
Filing Date:	20-FEB-2017
Time Stamp:	13:34:50
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$160
RAM confirmation Number	022218INTEFSW13344800
Deposit Account	132725
Authorized User	Julie Borrego

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

37 CFR 1.16 (National application filing, search, and examination fees)

37 CFR 1.17 (Patent application and reexamination processing fees)

37 CFR 1.19 (Document supply fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Terminal Disclaimer-Filed (Electronic)	eTerminal-Disclaimer.pdf	33587 ac8f582e64ca5e216f414b0f11498efbe042115d	no	2
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30777 a3ea81cb4388acd85c6b32bfdfeae5b02591c6a8	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	64364		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/437,275	02/20/2017	Joseph Jaroch	04584.0021USC1	4847

23552 7590 03/26/2018

MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

EXAMINER	
SHEHNI, GHAZAL B	

ART UNIT	PAPER NUMBER
2436	

NOTIFICATION DATE	DELIVERY MODE
03/26/2018	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

USPTO23552@merchantgould.com

Advisory Action Before the Filing of an Appeal Brief	**Application No.** 15/437,275	**Applicant(s)** JAROCH ET AL.	
	Examiner GHAZAL SHEHNI	**Art Unit** 2436	**AIA (First Inventor to File) Status** Yes

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 02/22/2018 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

NO NOTICE OF APPEAL FILED

1. ☒ The reply was filed after a final rejection. No Notice of Appeal has been filed. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114 if this is a utility or plant application. Note that RCEs are not permitted in design applications. The reply must be filed within one of the following time periods:
   a) ☒ The period for reply expires *3* months from the mailing date of the final rejection.
   b) ☐ The period for reply expires on: (1) the mailing date of this Advisory Action; or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.
   c) ☐ A prior Advisory Action was mailed more than 3 months after the mailing date of the final rejection in response to a first after-final reply filed within 2 months of the mailing date of the final rejection. The current period for reply expires months from the mailing date of *the prior Advisory Action* or SIX MONTHS from the mailing date of the final rejection, whichever is earlier.
   Examiner Note: If box 1 is checked, check either box (a), (b) or (c). ONLY CHECK BOX (b) WHEN THIS ADVISORY ACTION IS THE FIRST RESPONSE TO APPLICANT'S FIRST AFTER-FINAL REPLY WHICH WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. ONLY CHECK BOX (c) IN THE LIMITED SITUATION SET FORTH UNDER BOX (c). See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) or (c) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☐ The proposed amendments filed after a final rejection, but prior to the date of filing a brief, will not be entered because
   a) ☐ They raise new issues that would require further consideration and/or search (see NOTE below);
   b) ☐ They raise the issue of new matter (see NOTE below);
   c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.
   NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).
4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☐ Applicant's reply has overcome the following rejection(s): _____.
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☒ For purposes of appeal, the proposed amendment(s): (a) ☒ will not be entered, or (b) ☐ will be entered, and an explanation of how the new or amended claims would be rejected is provided below or appended.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.
9. ☐ The affidavit or other evidence filed after final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
10. ☐ The affidavit or other evidence filed after the date of filing the Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing of good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
11. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

12. ☐ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: _____.
13. ☐ Note the attached Information *Disclosure Statement*(s). (PTO/SB/08) Paper No(s). _____
14. ☒ Other: Examiner and Applicant's representative held multiple conversations regarding 112, 2nd paragraphs, and 101 rejections. The Applicant's representative would like more time for considering amendments overcoming 101 rejections. The Applicant's representative is invited to contact the Examiner with any further questions/clarifications.

STATUS OF CLAIMS

15. The status of the claim(s) is (or will be) as follows:
   Claim(s) allowed: .
   Claim(s) objected to: .
   Claim(s) rejected: 1-20

/GHAZAL SHEHNI/
Primary Examiner, Art Unit 2436

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Joseph Jaroch et al.	Examiner:	Shehni, Ghazal B.
Serial No.:	15/437,275	Group Art Unit:	2436
Filed:	February 20, 2017	Docket No.:	04584.0021USC1
Title:	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS		

RESPONSE TO FINAL OFFICE ACTION

Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Dear Commissioner:

In response to the Final Office Action mailed November 22, 2017, please amend the above-identified application as follows:

Remarks begin on page 2 of this paper.

DO NOT ENTER: /G.B.S/

/G.B.S/ (03/09/2018)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Joseph Jaroch et al.	Examiner:	Shehni, Ghazal B.
Serial No.:	15/437,275	Group Art Unit:	2436
Filed:	February 20, 2017	Docket No.:	04584.0021USC1
Title:	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS		

Filed via EFS-Web

REQUEST FOR CONTINUED EXAMINATION UNDER 37 C.F.R. §1.114

Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Dear Commissioner:

Under 37 C.F.R. § 1.114, it is respectfully requested that this application be accorded the benefits of Continued Examination. Please enter and consider the Amendment being filed concurrently herewith.

Payment in the amount of $1300 is being made via credit card to cover the required fee for a large entity. It is believed that no further fees are due with this request. However, the Commissioner is hereby authorized to charge any deficiencies or credit any overpayment with respect to this patent application to deposit account number 13-2725.

Respectfully submitted,

Date: April 23, 2018

/Ethan W. Bell/

Ethan W. Bell, Reg. No. 75,549
Merchant & Gould P.C.
P.O. Box 2903
Minneapolis, MN 55402-0903
(303) 357-1211

23552
PATENT TRADEMARK OFFICE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Joseph Jaroch et al.	Examiner:	Shehni, Ghazal B.
Serial No.:	15/437,275	Group Art Unit:	2436
Filed:	February 20, 2017	Docket No.:	04584.0021USC1
Title:	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS		

RESPONSE TO ADVISORY ACTION

Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Dear Commissioner:

In response to the Final Office Action mailed November 22, 2017, and the Advisory Action mailed March 26, 2018, please amend the above-identified application as follows:

Amendments to the Claims are reflected in the listing of claims that begins on page 2 of this paper.

Remarks begin on page 9 of this paper.

Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims:

1. (Previously Presented) A method comprising:

gathering an event defining an action of a first object acting on a target, wherein the first object is executed on a device;

generating contextual state information for the event by correlating the event to an originating object of the first object;

obtaining a global perspective for the event based on the contextual state information, wherein the global perspective comprises information associated with one or more of the first object and the originating object, and wherein the global perspective relates to one or more other events related to the event across a network;

generating an event line comprising information relating to the event, wherein the information relates to at least one of the first object, the action of the first object, the target, and the originating object; and

transmitting the generated event line.

2. (Original) The method of claim 1, wherein the information associated with the one or more of the first object and the originating object is obtained from a community database; and

wherein the event line is transmitted to an end recipient.

3. (Previously Presented) The method of claim 1, further comprising:

obtaining an event priority based on one or more of the generated contextual state information and the global perspective, wherein the event line further includes the event priority.

4. (Currently Amended) The method of claim 1, wherein the event includes information identifying the first object performing the action, information identifying the action being performed, and information identifying the target upon which the act is being performed.

5. (Previously Presented) The method of claim 4, further comprising:

determining whether the global perspective for the event has been cached;

when the global perspective for the event has been cached, obtaining the global perspective for the event based on the cached global perspective; and

when the global perspective for the event has not been cached, obtaining the global perspective for the event from a community database.

6. (Currently Amended) The method of claim 5, further comprising:

determining whether the cached global perspective for the event has expired, based on a time-to-live value associated with the cached global perspective; and

when the global perspective for the event has expired, obtaining the global perspective for the event from [[a]] the community database.

7. (Currently Amended) The method of claim 4, further comprising:

heuristically displaying the information identifying the first object performing the action, the information identifying the action being performed, the information identifying the target upon which the act is being performed, and information associated with the global perspective according to one or more of:

a location associated with the first object;

at least one characteristic of an outbound connection associated with the first object;

a dropped executable file;

an age of the first object; and

a number of concurrent connections associated with the first object.

8. (Currently Amended) The method of claim 1, wherein the global perspective comprises information comprises ~~including~~ at least one of:

an age;

a popularity;

a determination as to whether the first object is malware;

a determination as to whether the originating object is malware;

an Internet Protocol (IP) Address; and

a Uniform Resource Locator (URL).

9. (Currently Amended) A system for providing forensic visibility into a system, comprising:

a device ~~including~~ comprising:

a communication interface;

a processor;

data storage; and

a sensor agent stored on the data storage that is executable by the processor, wherein the sensor agent is operable to:

gather an event defining an action of a first object acting on a target;

generate contextual state information for the event by correlating the event to an originating object of the first object;

obtain a global perspective for the event based on the contextual state information, wherein the global perspective comprises information associated with one or more of the first object and the originating object, and wherein the global perspective relates to one or more other events related to the event across a network;

generate an event line comprising information relating to the event, wherein the information relates to at least one of the first object, the action of the first object, the target, and the originating object; and

transmit the generated event line utilizing the communication interface.

10. (Previously Presented) The system of claim 9, wherein the event is executed by the processor.

11. (Previously Presented) The system of claim 9, further comprising:

a global perspective information server; and

an end recipient device, wherein the information associated with the one or more of the first object and the originating object is obtained from the global perspective information server and the sensor agent transmits the event line to the end recipient device.

12. (Previously Presented) The system of claim 8, wherein the sensor agent is further operable to:

cache the event and one or more other events; and

asynchronously consolidate and normalize the event and the one or more other events.

13. (Currently Amended) The system of claim 9, wherein the event includes information identifying the first object performing the action, information identifying the action being performed, and information identifying the target upon which the act is being performed.

14. (Previously Presented) The system of claim 13, wherein the sensor agent is further operable to:

determine whether the global perspective for the event has been cached;

when the global perspective for the event has been cached, obtain the global perspective for the event based on the cached global perspective; and

when the global perspective for the event has not been cached, obtain the global perspective for the event from a community database.

15. (Currently Amended) The system of claim 14, wherein the sensor agent is further operable to:

determine whether the cached global perspective for the event has expired, based on a time-to-live value associated with the cached global perspective; and

when the global perspective for the event has expired, obtain the global perspective for the event from [[a]] the community database.

16. (Currently Amended) The system of claim 13 [[11]], wherein the end recipient device heuristically displays the information identifying the first object performing the action, the information identifying the action being performed, the information identifying the target upon which the act is being performed, and information associated with the global perspective according to one or more of:

a location associated with the first object;

at least one characteristic of an outbound connection associated with the first object;

a dropped executable file;

an age of the first object; and

a number of concurrent connections associated with the first object.

17. (Currently Amended) A system for providing forensic visibility into a system, comprising:

a first device ~~including~~ comprising:

a communication interface;

a processor;

data storage; and

a sensor agent stored on the data storage that is executable by the processor, wherein the sensor agent is operable to:

gather an event defining an action of a first object acting on a target;

determine a global perspective for the event based on contextual state information for the event, wherein the global perspective relates to one or more other events related to the event across a network, and wherein the contextual state comprises an indication of an originating object of the first object and an indication of at least one of a second device on which the first object is executed and a user associated with the first object;

generate an event line comprising information relating to the event, wherein the information relates to at least one of the first object, the action of the first object, the target, and the originating object; and

transmit the generated event line utilizing the communication interface.

18. (Currently Amended) The system of claim 17, further comprising a global perspective information server ~~including~~ comprising:

a processor;

a communication interface;

data storage; and

a global perspective module, wherein the global perspective module is operable to:

receive the event line from the device;

assemble a second event line including details associated with the event, wherein the second event line comprises information identifying ~~each of~~ the first object, information identifying the action of the first object, information identifying the target, and information identifying the originating object; and

transmit the second event line utilizing the communication interface to an end recipient.

19. (Currently Amended) The system of claim 18, wherein the end recipient heuristically displays the information identifying the first object ~~performing the action~~, the information identifying the action of the first object ~~being performed~~, the information identifying the target ~~upon which the act is being performed~~, and information associated with the global perspective according to one or more of:

a location associated with the first object;

at least one characteristic of an outbound connection associated with the first object;

a dropped executable file;

an age of the first object; and

a number of concurrent connections associated with the first object.

20. (Currently Amended) The system of claim 17, further comprising a bridge ~~including~~ comprising:

a processor;

a communication interface; and

a cached event store, wherein the cached event store is operable to:

receive a first request for a global perspective for the event;

receive a second request for a global perspective for another event, the second request originating from another device;

obtain a first global perspective for the event by obtaining information associated with one or more of the first object and the originating object;

obtain a second global perspective for the another event;

provide the first global perspective to the device; and

provide the second global perspective to the another device.

REMARKS

This Amendment and the following remarks are intended to fully respond to the final Office Action dated November 22, 2017, hereinafter "Office Action." In that Office Action, claims 1-20 were examined and all claims were rejected.

Double Patenting Rejection

Claims 1-20 were rejected on the ground of nonstatutory double patenting over U.S. Patent No. 9,578,045. Applicants have filed a terminal disclaimer over Patent No. 9,578,045, dated February 22, 2018. Accordingly, the rejection is obviated and Applicants respectfully request withdrawal of the rejection and allowance of claims 1-20 at the Examiner's earliest convenience.

Interview Summary

Applicants thank Examiner Ghazal Shehni for the courtesy of multiple telephone interviews, conducted on February 28, 2018 and April 23, 2018, with Applicant's representatives, Attorney Andrew Pouzeshi (Reg. No. 67,672) and Attorney Ethan Bell (Reg. No. 75,549). During the interviews, various claim informalities were discussed, as well as a potential rejection under 35 U.S.C. § 101. By the present amendment, Applicants respectfully submit the informalities discussed during the interviews have been corrected. No agreement as to the ultimate allowability of the claims was reached.

CONCLUSION

This Amendment fully responds to the Office Action mailed on November 22, 2017. Still, that Office Action may contain arguments and rejections that are not directly addressed by this Amendment due to the fact that they are rendered moot in light of the preceding arguments in favor of patentability. Hence, the failure, if any, of this Amendment and Response to directly address an argument and/or comment raised in the Office Action should not be taken as an indication that the Applicants believe the argument and/or comment has merit. Additionally, the failure, if any, to address statements and/or comments made in the Office Action does not mean that the Applicants acquiesce to such statements and/or comments. Furthermore, the claims of the present application may include other elements, not discussed in this Amendment and Response, which are not shown, taught, or otherwise suggested by the art of record. Accordingly, the preceding arguments in favor of patentability are advanced without prejudice to other bases of patentability.

This Amendment is filed concurrently with a Request for Continued Examination and Petition for Extension of Time. It is believed that no further fees are due with this Response. However, the Commissioner is hereby authorized to charge any deficiencies or credit any overpayment with respect to this patent application to deposit account number 13-2725.

In light of the above remarks and amendments, it is believed that the application is now in condition for allowance and such action is respectfully requested. Should any additional issues need to be resolved, the Examiner is requested to telephone the undersigned to attempt to resolve those issues.

Respectfully submitted,

Date: April 23, 2018

/Ethan W. Bell/

Ethan W. Bell, Reg. No. 75,549
Merchant & Gould P.C.
P.O. Box 2903
Minneapolis, MN 55402-0903
(303) 357-1211

27488
PATENT TRADEMARK OFFICE

PTO/AIA/22 (03-13)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)

Docket Number (Optional): 04584.0021USC1

Application Number: 15/437,275

Filed: February 20, 2017

For: METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS

Art Unit: 2436

Examiner: Shehni, Ghazal B.

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above-identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

	Fee	Small Entity Fee	Micro Entity Fee	
☐ One month (37 CFR 1.17(a)(1))	$200	$100	$50	$
☑ Two months (37 CFR 1.17(a)(2))	$600	$300	$150	$ 600
☐ Three months (37 CFR 1.17(a)(3))	$1,400	$700	$350	$
☐ Four months (37 CFR 1.17(a)(4))	$2,200	$1,100	$550	$
☐ Five months (37 CFR 1.17(a)(5))	$3,000	$1,500	$750	$

☐ Applicant asserts small entity status. See 37 CFR 1.27.

☐ Applicant certifies micro entity status. See 37 CFR 1.29.
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

☐ A check in the amount of the fee is enclosed.

☑ Payment by credit card. ~~Form PTO-2038 is attached.~~

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☑ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 13-2725.

☑ Payment made via EFS-Web.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant.

☑ attorney or agent of record. Registration number 75,549.

☐ attorney or agent acting under 37 CFR 1.34. Registration number _____.

/Ethan W. Bell/ — Signature

2018-04-23 — Date

Ethan W. Bell — Typed or printed name

303-357-1211 — Telephone Number

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☑ * Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.136(a). The information is required to obtain or retain a benefit by the public, which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 6 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop PCT, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Electronic Patent Application Fee Transmittal

Application Number:	15437275
Filing Date:	20-Feb-2017
Title of Invention:	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS
First Named Inventor/Applicant Name:	Joseph Jaroch
Filer:	Ethan Wendel Bell/Julie Borrego
Attorney Docket Number:	04584.0021USC1

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 2 months with $0 paid	1252	1	600	600
Miscellaneous:				
RCE- 1ST REQUEST	1801	1	1300	1300
		Total in USD ($)		**1900**

Electronic Acknowledgement Receipt

EFS ID:	32414570
Application Number:	15437275
International Application Number:	
Confirmation Number:	4847
Title of Invention:	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS
First Named Inventor/Applicant Name:	Joseph Jaroch
Customer Number:	23552
Filer:	Ethan Wendel Bell/Julie Borrego
Filer Authorized By:	Ethan Wendel Bell
Attorney Docket Number:	04584.0021USC1
Receipt Date:	23-APR-2018
Filing Date:	20-FEB-2017
Time Stamp:	15:17:05
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$1900
RAM confirmation Number	042418INTEFSW15174600
Deposit Account	132725
Authorized User	Julie Borrego

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

37 CFR 1.16 (National application filing, search, and examination fees)

37 CFR 1.17 (Patent application and reexamination processing fees)

37 CFR 1.19 (Document supply fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request for Continued Examination (RCE)	2018_04_23_RCE_04584_0021 USC1.pdf	82078 a438583adce29da7d464488fe4a5039bf3645633	no	1
Warnings:					
This is not a USPTO supplied RCE SB30 form.					
Information:					
2		2018_04_23_RESP_AA_04584_0021USC1.pdf	106891 fac5fcfa6c0e840d299c897637fc65245fb2e1b7	yes	10

Multipart Description/PDF files in .zip description		
Document Description	**Start**	**End**
Amendment Submitted/Entered with Filing of CPA/RCE	1	1
Claims	2	8
Applicant Arguments/Remarks Made in an Amendment	9	10

Warnings:					
Information:					
3	Extension of Time	2018_04_23_EOT_04584_0021 USC1.pdf	126541 5c6403c7315fcbbd7ec75c4fbfd36019803875aa	no	1
Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	32917 62ec4cef9419c128067102f92102d8935bc68403	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	348427		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 15/437,275	Filing Date 02/20/2017	☐ To be Mailed

ENTITY: ☑ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A		N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A		N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*		x $80 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*		x $420 =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).				
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))					
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT	04/23/2018	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 20	Minus	** 20	= 0		x $100 =	0
	Independent (37 CFR 1.16(h))	* 3	Minus	*** 3	= 0		x $460 =	0
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	0

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=		x $ 0 =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=		x $ 0 =	
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.	LIE
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".	tina J barden
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".	
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.	

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/437,275	02/20/2017	Joseph Jaroch	04584.0021USC1	4847

23552 7590 05/29/2018

MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MINNESOTA 55402-0903
UNITED STATES OF AMERICA

EXAMINER
SHEHNI, GHAZAL B

ART UNIT	PAPER NUMBER
2436	

NOTIFICATION DATE	DELIVERY MODE
05/29/2018	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

USPTO23552@merchantgould.com

Office Action Summary	Application No. 15/437,275	Applicant(s) Jaroch et al.	
	Examiner GHAZAL B SHEHNI	Art Unit 2436	AIA Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☑ Responsive to communication(s) filed on 04/23/2018.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL.** 2b) ☑ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5) ☑ Claim(s) 1-20 is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 1-4,7-11,13 and 16-20 is/are rejected.

8) ☑ Claim(s) 5-6,12 and 14-15 is/are objected to.

9) ☐ Claim(s) _____ are subject to restriction and/or election requirement

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to **PPHfeedback@uspto.gov.**

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☑ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date 02/22/2018.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.

4) ☐ Other: _____.

Notice of Pre-AIA or AIA Status

The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 04/23/2018 has been entered.

The following is a non-final office action in response to communications received 04/23/2018 Claims 1-20 are pending and addressed below.

Examiner's note

Examiner contacted the Applicant's representative on 05/23/2018 to discuss the 35 USC 101 rejections. Applicant's representative request for the non-final rejection office action to be issued.

Allowable Subject Matter

Claims 5-6, 12, 14-15 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Claim Rejections - 35 USC § 101

1. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-4, 7-11, 13, 16-20 are rejected under 35 U.S.C. 101 because the claimed invention is directed to a judicial exception (i.e., a law of nature, a natural phenomenon, or an abstract idea) without significantly more.

Claims 1, 9, 17 recite steps of calculating, and generating. These steps are directed to an idea of itself and are similar to concepts identified as abstract idea by the courts (e.g. Collecting and analyzing information to detect misuse and notifying a user when misuse is detected (FairWarning); Collecting, displaying, and manipulating data (Int. Ventures v. Cap One Financial); Collecting information, analyzing it, and displaying certain results of the collection and analysis (Electric Power Group)). The claim elements in addition to the abstract idea are: a device, a communication interface, a processor, data storage. However, the device, the communication interface, the processor, the data storage are recited at a high level of generality to simply perform the generic computer functions of generating, obtaining, transmitting. Generic computers performing generic computer functions, alone, do not amount to significantly more than the

abstract idea. Viewing the elements as a combination does not add anything further than the individual elements. Viewing the elements of Dependent claims 2-7, 9-14, 16-21 as a combination does not add anything further than the individual elements. Therefore Examiner maintains the 101 rejections as set forth in the previous office action.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to GHAZAL B SHEHNI whose telephone number is (571)270-7479. The examiner can normally be reached on Mon-Fri 9am-3pm; 6-8pm PCT.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Shewaye Gelagay can be reached on 5712724219. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/GHAZAL B SHEHNI/
Primary Examiner, Art Unit 2436

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/437,275	Jaroch et al.
	Examiner	Art Unit
	GHAZAL B SHEHNI	2436

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	03/28/2017	11/17/2017	05/23/2018						
	1	✓	✓	✓						
	2	✓	✓	✓						
	3	✓	✓	✓						
	4	✓	✓	✓						
	5	✓	✓	O						
	6	✓	✓	O						
	7	✓	✓	✓						
	8	✓	✓	✓						
	9	✓	✓	✓						
	10	✓	✓	✓						
	11	✓	✓	✓						
	12	✓	✓	O						
	13	✓	✓	✓						
	14	✓	✓	O						
	15	✓	✓	O						
	16	✓	✓	✓						
	17	✓	✓	✓						
	18	✓	✓	✓						
	19	✓	✓	✓						
	20	✓	✓	✓						

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/437,275	Jaroch et al.
	Examiner	Art Unit
	GHAZAL B SHEHNI	2436

CPC - Searched*		
Symbol	Date	Examiner
H04L63/1416 OR H04L63/20 OR H04L63/1425 OR H04L63/1441 OR H04L63/1408 OR H04L63/1433 OR H04L63/145 OR H04L63/14 OR H04L9/3271 OR H04L12/2602	3/28/2017	GS

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
Inventor search (see search history printout)	3/28/2017	GS
East (see search history printout)	3/28/2017	GS
CPC with text search	3/28/2017	GS
East (see search history printout)	11/17/2017	GS
East (see search history printout)	05/23/2018	GS

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

/GHAZAL B SHEHNI/ Primary Examiner, Art Unit 2436	

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (03-15)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	15437275
Filing Date	2017-02-20
First Named Inventor	Joseph JAROCH
Art Unit	2436
Examiner Name	Shehni, Ghazal B.
Attorney Docket Number	04584.0021USC1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	15437275
Filing Date	2017-02-20
First Named Inventor	Joseph JAROCH
Art Unit	2436
Examiner Name	Shehni, Ghazal B.
Attorney Docket Number	04584.0021USC1

/G.B.S/	1	European Office Action in Application 14791882.5, mailed 2017-12-08, 6 pages.

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/GHAZAL B SHEHNI/	Date Considered	05/23/2018

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	15437275
Filing Date	2017-02-20
First Named Inventor	Joseph JAROCH
Art Unit	2436
Examiner Name	Shehni, Ghazal B.
Attorney Docket Number	04584.0021USC1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

X That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

X See attached certification statement.

X The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Ethan W. Bell/	Date (YYYY-MM-DD)	2018-02-22
Name/Print	Ethan W. Bell	Registration Number	75,549

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /G.B.S/

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	10	(("JAROCH") near3 ("Joseph")).INV.	US-PGPUB; USPAT; USOCR	ADJ	ON	2017/03/27 20:14
S2	3	(("ERASMUS") near3 ("Jacques")).INV.	US-PGPUB; USPAT; USOCR	ADJ	ON	2017/03/27 20:14
S3	63	(("BARNES") near3 ("Paul")).INV.	US-PGPUB; USPAT; USOCR	ADJ	ON	2017/03/27 20:14
S4	9	(("MAYR") near3 ("Johannes")).INV.	US-PGPUB; USPAT; USOCR	ADJ	ON	2017/03/27 20:15
S5	2	(("LEIDESDORFF") near3 ("Michael")).INV.	US-PGPUB; USPAT; USOCR	ADJ	ON	2017/03/27 20:15
S6	16	(("GIULIANI") near3 ("Marco")).INV.	US-PGPUB; USPAT; USOCR	ADJ	ON	2017/03/27 20:15
S7	1533	(("WILLIAMS") near3 ("Christopher")).INV.	US-PGPUB; USPAT; USOCR	ADJ	ON	2017/03/27 20:15
S8	2	(("BACHER") near3 ("Chad")).INV.	US-PGPUB; USPAT; USOCR	ADJ	ON	2017/03/27 20:15
S9	880	(virus or malicious or trojan or spy$ware or mal$ware) with ((analyz$3 or analys$3 or determin$5 or detect$4) with (security with event))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/28 14:17
S10	21	(virus or malicious or trojan or spy$ware or mal$ware) with (((analyz$3 or analys$3 or determin$5 or detect$4) with forensic) with (security with (behavior or pattern or event)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/28 14:22
S11	17254	(analys$3 or analyz$3 or detect$4 or monitor$3 or record$3 or captur$3) with ((security with attack) or (network with attack))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/28 14:26
S12	213	(analys$3 or analyz$3 or detect$4 or monitor$3 or record$3 or captur$3) with ((security with attack) or (network with attack)) with forensic	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/28 14:26

S13	111	S12 AND ((H04L63/1416 OR H04L63/20 OR H04L63/1425 OR H04L63/1441 OR H04L63/1408 OR H04L63/1433 OR H04L63/145 OR H04L63/14 OR H04L9/3271 OR H04L12/2602).CPC.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/28 14:29
S14	1	("20130298244").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2017/03/28 14:32

EAST Search History (Interference)

< This search history is empty>

5/ 23/ 2018 5:16:16 PM
C:\ Users\ gshehni\ Documents\ EAST\ Workspaces\ 15437275.wsp

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Joseph Jaroch et al.	Examiner:	Shehni, Ghazal B.
Serial No.:	15/437,275	Group Art Unit:	2436
Filed:	February 20, 2017	Docket No.:	04584.0021USC1
Title:	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS		

RESPONSE TO NON-FINAL OFFICE ACTION

Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Dear Commissioner:

In response to the Non-Final Office Action mailed May 29, 2018, please consider the following:

Listing of Claims begins on page 2 of this paper.

Remarks begin on page 9 of this paper.

Listing of Claims:

1. (Previously Presented) A method comprising:

gathering an event defining an action of a first object acting on a target, wherein the first object is executed on a device;

generating contextual state information for the event by correlating the event to an originating object of the first object;

obtaining a global perspective for the event based on the contextual state information, wherein the global perspective comprises information associated with one or more of the first object and the originating object, and wherein the global perspective relates to one or more other events related to the event across a network;

generating an event line comprising information relating to the event, wherein the information relates to at least one of the first object, the action of the first object, the target, and the originating object; and

transmitting the generated event line.

2. (Original) The method of claim 1, wherein the information associated with the one or more of the first object and the originating object is obtained from a community database; and

wherein the event line is transmitted to an end recipient.

3. (Previously Presented) The method of claim 1, further comprising:

obtaining an event priority based on one or more of the generated contextual state information and the global perspective, wherein the event line further includes the event priority.

4. (Previously Presented) The method of claim 1, wherein the event includes information identifying the first object performing the action, information identifying the action being performed, and information identifying the target upon which the act is being performed.

5. (Previously Presented) The method of claim 4, further comprising:

determining whether the global perspective for the event has been cached;

when the global perspective for the event has been cached, obtaining the global perspective for the event based on the cached global perspective; and

when the global perspective for the event has not been cached, obtaining the global perspective for the event from a community database.

6. (Previously Presented) The method of claim 5, further comprising:

determining whether the cached global perspective for the event has expired, based on a time-to-live value associated with the cached global perspective; and

when the global perspective for the event has expired, obtaining the global perspective for the event from the community database.

7. (Previously Presented) The method of claim 4, further comprising:

heuristically displaying the information identifying the first object performing the action, the information identifying the action being performed, the information identifying the target upon which the act is being performed, and information associated with the global perspective according to one or more of:

a location associated with the first object;

at least one characteristic of an outbound connection associated with the first object;

a dropped executable file;

an age of the first object; and

a number of concurrent connections associated with the first object.

8. (Previously Presented) The method of claim 1, wherein the global perspective comprises information comprises at least one of:

an age;

a popularity;

a determination as to whether the first object is malware;

a determination as to whether the originating object is malware;

an Internet Protocol (IP) Address; and

a Uniform Resource Locator (URL).

9. (Previously Presented) A system for providing forensic visibility into a system, comprising:

a device comprising:

a communication interface;

a processor;

data storage; and

a sensor agent stored on the data storage that is executable by the processor, wherein the sensor agent is operable to:

gather an event defining an action of a first object acting on a target;

generate contextual state information for the event by correlating the event to an originating object of the first object;

obtain a global perspective for the event based on the contextual state information, wherein the global perspective comprises information associated with one or more of the first object and the originating object, and wherein the global perspective relates to one or more other events related to the event across a network;

generate an event line comprising information relating to the event, wherein the information relates to at least one of the first object, the action of the first object, the target, and the originating object; and

transmit the generated event line utilizing the communication interface.

10. (Previously Presented) The system of claim 9, wherein the event is executed by the processor.

11. (Previously Presented) The system of claim 9, further comprising:

a global perspective information server; and

an end recipient device, wherein the information associated with the one or more of the first object and the originating object is obtained from the global perspective information server and the sensor agent transmits the event line to the end recipient device.

12. (Previously Presented) The system of claim 8, wherein the sensor agent is further operable to:

cache the event and one or more other events; and

asynchronously consolidate and normalize the event and the one or more other events.

13. (Previously Presented) The system of claim 9, wherein the event includes information identifying the first object performing the action, information identifying the action being performed, and information identifying the target upon which the act is being performed.

14. (Previously Presented) The system of claim 13, wherein the sensor agent is further operable to:

determine whether the global perspective for the event has been cached;

when the global perspective for the event has been cached, obtain the global perspective for the event based on the cached global perspective; and

when the global perspective for the event has not been cached, obtain the global perspective for the event from a community database.

15. (Previously Presented) The system of claim 14, wherein the sensor agent is further operable to:

determine whether the cached global perspective for the event has expired, based on a time-to-live value associated with the cached global perspective; and

when the global perspective for the event has expired, obtain the global perspective for the event from the community database.

16. (Previously Presented) The system of claim 13, wherein the end recipient device heuristically displays the information identifying the first object performing the action, the

information identifying the action being performed, the information identifying the target upon which the act is being performed, and information associated with the global perspective according to one or more of:

a location associated with the first object;

at least one characteristic of an outbound connection associated with the first object;

a dropped executable file;

an age of the first object; and

a number of concurrent connections associated with the first object.

17. (Previously Presented) A system for providing forensic visibility into a system, comprising:

a first device comprising:

a communication interface;

a processor;

data storage; and

a sensor agent stored on the data storage that is executable by the processor, wherein the sensor agent is operable to:

gather an event defining an action of a first object acting on a target;

determine a global perspective for the event based on contextual state information for the event, wherein the global perspective relates to one or more other events related to the event across a network, and wherein the contextual state comprises an indication of an originating object of the first object and an indication of at least one of a second device on which the first object is executed and a user associated with the first object;

generate an event line comprising information relating to the event, wherein the information relates to at least one of the first object, the action of the first object, the target, and the originating object; and

transmit the generated event line utilizing the communication interface.

18. (Previously Presented) The system of claim 17, further comprising a global perspective information server comprising:

a processor;

a communication interface;

data storage; and

a global perspective module, wherein the global perspective module is operable to:

receive the event line from the device;

assemble a second event line including details associated with the event, wherein the second event line comprises information identifying the first object, information identifying the action of the first object, information identifying the target, and information identifying the originating object; and

transmit the second event line utilizing the communication interface to an end recipient.

19. (Previously Presented) The system of claim 18, wherein the end recipient heuristically displays the information identifying the first object, the information identifying the action of the first object, the information identifying the target, and information associated with the global perspective according to one or more of:

a location associated with the first object;

at least one characteristic of an outbound connection associated with the first object;

a dropped executable file;

an age of the first object; and

a number of concurrent connections associated with the first object.

20. (Previously Presented) The system of claim 17, further comprising a bridge comprising:

a processor;

a communication interface; and

a cached event store, wherein the cached event store is operable to:

receive a first request for a global perspective for the event;

receive a second request for a global perspective for another event, the second request originating from another device;

obtain a first global perspective for the event by obtaining information associated with one or more of the first object and the originating object;

obtain a second global perspective for the another event;

provide the first global perspective to the device; and

provide the second global perspective to the another device.

REMARKS/ARGUMENTS

This Response is intended to fully respond to the non-final Office Action dated May 29, 2018, hereinafter "Office Action." In that Office Action, claims 1-20 were examined, claims 1-4, 7-11, 13, and 16-20 were rejected and claims 5-6, 12, and 14-15 were objected to. Specifically, claims 1-4, 7-11, 13, and 16-20 were rejected under 35 U.S.C. § 101 for allegedly being directed to a judicial exception (i.e., a law of nature, a natural phenomenon, or an abstract idea) without significantly more.

Reconsideration of these rejections, as they might apply to the claims in view of these remarks, is respectfully requested. In this Response, no claims have been amended, no claims have been canceled without prejudice, and no claims have been added. Therefore, claims 1-20 remain present for examination.

Allowable Subject Matter

Applicant acknowledges with appreciation the Examiner's identification of claims 5-6, 12, and 14-15 as allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims. Applicant respectfully submits that, for at least the reasons set forth below, the other claims are similarly allowable. Accordingly, Applicant respectfully requests withdrawal of the objections and allowance of claims 5-6, 12, and 14-15 at the Examiner's earliest convenience.

Claim Rejections under 35 U.S.C. § 101

Claims 1-4, 7-11, 13, and 16-20 were rejected under 35 U.S.C. § 101 for allegedly being directed to a judicial exception (i.e., a law of nature, a natural phenomenon, or an abstract idea) without significantly more. More specifically, the Office Action alleges the claims "recite steps of calculating, and generating." Office Action, pg. 3. The Office Action then compares the alleged abstract idea to:

> Collecting and analyzing information to detect misuse and notifying a user when misuse is detected (FairWarning); Collecting, displaying, and manipulating data (Int. Ventures v. Cap One Financial), Collecting information, analyzing it, and displaying certain results of the collection and analysis (Electric Power Group).

Office Action, pg. 3.

The Office Action then identifies the additional elements, which are said to be "a device, a communication interface, a processor, data storage." Office Action, pg. 3. However, these elements are allegedly "recited at a high level of generality to simply perform the generic computer functions of generating, obtaining, transmitting." Office Action, pg. 3. As a result, it is concluded that such elements "do not amount to significantly more than the abstract idea" and, further, that "viewing the elements as a combination does not add anything further than the individual elements." Office Action, pgs. 3-4. Applicant respectfully disagrees.

Rather, Applicant respectfully submits that the instant claims are directed to improvements in computer functionality and are therefore not abstract. For example, MPEP § 2106.04(a)(I) indicates that "some inventions pertaining to improvements in computer functionality or to improvements in other technologies are not abstract when appropriately claimed, and thus may be eligible at Step 2A." More specifically:

> When finding that a claim is directed to such an improvement, it is critical that examiners give the claim its broadest reasonable interpretation (BRI) and evaluate both the specification and the claim. The specification should disclose sufficient details such that one of ordinary skill in the art would recognize the claimed invention as providing an improvement, and the claim itself must reflect the improvement in technology. Other important considerations are the extent to which the claim covers a particular solution to a problem or a particular way to achieve a desired outcome, as opposed to merely claiming the idea of a solution or outcome, and whether the BRI is limited to computer implementation.

MPEP § 2106.04(a)(I).

Here, the claims are directed to a specific improvement in computer functionality relating to computer security, and more specifically to providing end-to-end visibility of events within a system and/or network. Further, Applicant respectfully submits that the Specification provides sufficient details to enable one of ordinary skill in the art to recognize the claimed invention as providing an improvement. *See* MPEP § 2106.04(a)(I). For example, the Specification details example aspects of the problems addressed by the claimed solution as follows:

> [0004] **However, existing network forensic tools, such as network sniffers and packet capturing tools, passively collect information about network traffic.** Such tools may be able to detect and capture information associated with communication sessions, such as hostnames, ports, protocols, IP addresses, etc.;

> **however, such tools tend to receive network events outside of a host or system. That is, a network forensic tool, such as a network sniffer, may reside at a network edge and may receive network events concerning the network from one or more hosts or systems. Accordingly, network edge devices have no ability to establish any sort of context from within the host or system that is generating the event.** Therefore, devices residing at a network edge may monitor, record, and or analyze network traffic between the host and the device, but information that may be useful within the host is not obtained.
>
> . . .
>
> [0006] However, as previously mentioned, the **network edge device 116 has no ability to monitor, capture, and/or analyze what is occurring within each of the computing device 104 and 108.** In at least one comparative example, computing device 108 may contain or otherwise be infected with one or more pieces of malware. The term "malware" is used herein to refer generally to any executable computer file or, more generally "object", that is or contains malicious code, and thus includes viruses, Trojans, worms, spyware, adware, etc. and the like. Indeed, the network edge device 116 may be able to monitor, capture, and analyze communication traffic including the information, both encrypted and unencrypted, source and destination ports, source and destination IP address, and protocols utilized by the computing device 108, but the network edge device cannot provide details regarding files modified, registry entries changed, and/or new processes that are created. **Accordingly, the network edge device 116 has no way of knowing to what extent the virus may have impacted the computing device 108, what additional files may have become infected, or what processes and/or objects operating are linked to the virus. What is needed therefore, is a solution that eliminates the guesswork and allows for end-to-end visibility of every event within a system and/or within a network.**

Specification, paras. [0004]-[0006] (emphasis added).

The Specification subsequently discusses a variety of ways in which the claimed subject matter solves the above-described problem. For example:

> It is, therefore, one aspect of the present disclosure to **provide a system and method whereby events occurring within a computing device are captured and additional context and a global perspective is provided for each capture event.** For example, a sensor agent may provide **visibility into occurrences across an environment, such as a networked environment, to ensure that an administrator is aware of any system changes and data communication in and out of computing devices residing on the network.** In this implementation, six components, or modules, may be utilized in the event gathering and processing: low level system filters, a local aggregator and interpreter, a context analyzer, a global perspective module, an event priority module, and an event

> distributor may be utilized to provide forensic visibility into one or more computing devices of a communication network.

Specification, para. [0007] (emphasis added).

Additionally, not only does the disclosed invention improve technology, as detailed by the Specification in at least the paragraphs cited above, but the claims also cover a particular solution to the disclosed problem and a particular way to achieve a desired outcome. *See* MPEP § 2106.04(a)(I). For instance, claim 1 recites, *inter alia*, "gathering an event defining an action of a first object acting on a target, wherein the first object is executed on a device," "generating contextual state information for the event by correlating the event to an originating object of the first object," "obtaining a global perspective for the event based on the contextual state information, wherein the global perspective comprises information associated with one or more of the first object and the originating object, and wherein the global perspective relates to one or more other events related to the event across a network," "generating an event line comprising information relating to the event, wherein the information relates to at least one of the first object, the action of the first object, the target, and the originating object," and "transmitting the generated event line."

Thus, Applicant respectfully submits that such claim language does not "merely [claim] the idea of a solution or outcome," but rather sets forth "a particular solution to a problem or a particular way to achieve a desired outcome." MPEP § 2106.04(a)(I). Specifically, the claims focus on the particular solution and the particular way to achieve the desired outcome as described by at least the aspects in the above-quoted paragraphs of the Specification. Further, the broadest reasonable interpretation of the claims is limited to a computer implementation, as illustrated at least by the claimed "gathering an event defining an action of a first object acting on a target, wherein the first object is executed on a device," "generating contextual state information for the event," "obtaining a global perspective for the event based on the contextual state information," and "generating an event line comprising information relating to the event." Indeed, computer security technology is necessarily rooted in computer technology, and, accordingly, the claimed improvement to computer security technology is similarly rooted in computer technology.

In support of the conclusion that the instant claims are directed to an abstract idea, the Office Action cites to *FairWarning*, *Capital One Financial*, and *Electric Power Group*. Specifically, the Office Action overgeneralizes the claims as "recit[ing] steps of calculating, and generating," and likens such steps to "collecting and analyzing information," "collecting, displaying, and manipulating data," and "collecting information, analyzing it, and displaying certain results." Office Action, pg. 3.

The court in *FairWarning* found the claims at issue to be abstract, as they were "directed to or drawn to the concept of analyzing records of human activity to detect suspicious behavior," and were "not directed to an improvement in the way computers operate." *FairWarning IP, LLC v. Iatric Sys.*, 839 F.3d 1089, 1093, 1095 (Fed. Cir. 2016). Rather, the claims "merely implement[ed] an old practice in a new environment." *FairWarning*, at 1094. The claims at issue in *Capital One Financial* were found to be directed toward "a system and method for editing XML documents." *Intellectual Ventures I LLC v. Capital One Fin. Corp.*, 850 F.3d 1332, 1339 (Fed. Cir. 2017). However, the court concludes that "the patent's recitation of XML documents specifically, does little more than restrict the invention's field of use. Such limitations do not render an otherwise abstract concept any less abstract." *Capital One Financial*, at 1340. Similar to *FairWarning*, the court ultimately concludes that the claimed subject matter fails to improve a technological process. *See Capital One Financial*, at 1341. Finally, the Office Action also cites to *Electric Power Group*, where the Federal Circuit based its opinion on the finding that "the focus of the claims **is not on such an improvement in computers as tools, but on certain independently abstract ideas that use computers as tools**." *Elec. Power Grp., LLC v. Alstom S.A.*, 830 F.3d 1350, 1354 (Fed. Cir. 2016) (emphasis added).

However, Applicant respectfully submits that the present case is in contrast to the cases cited by the Office Action. Indeed, the claims do not merely recite implementing "an old practice in a new environment" or "limit[] the invention to a technological environment for which to apply the underlying abstract concept," as was the case in *FairWarning* and *Capital One Financial*. Further, the claims do not merely "use computers as tools," as was the case in *Electric Power Group*. Rather, the present claims instead recite an improvement in the way computers operate, and relate to a specific improvement in the functioning of computers as tools. For

example, as discussed above, the present technology provides for improved computer functionality relating to computer security, and more specifically to providing end-to-end visibility of events within a system and/or network. Thus, in contrast to the cases cited by the Office Action, the present claims improve computing technology.

Further, Applicant respectfully submits that the characterizations of the claimed subject matter set forth by the Office Action (e.g., "steps of calculating, and generating," Office Action, pg. 3) vastly oversimplify the claimed invention in a manner that has been explicitly admonished by the Federal Circuit, which has stated that "describing the claims at such a high level of abstraction and untethered from the language of the claims all but ensures that the exceptions to § 101 swallow the rule." *Enfish*, 822 F.3d at 1337. In fact, the PTAB recently reversed a rejection under 35 U.S.C. § 101 of claims that were allegedly directed to the abstract idea of "generic audio analysis." The PTAB concluded that the Examiner's summary "oversimplifie[d] the claims and fail[ed] to account for the specific requirements of capturing only a single frame from each block, analyzing the collection of captured frames, and determining a characteristic of an ambient environment based on that analysis." *Ex parte Grokop*, Appeal 2016-003047, at 4 (PTAB Sept. 14, 2017).

The characterizations set forth in the Office Action and the resulting rejections are similarly untethered from the language of the instant claims. The claims do not merely "recite steps of calculating, and generating," as is alleged by the Office Action. Office Action, pg. 3. Rather, claim 1 is deeply rooted in technology and includes specific elements directed toward, *inter alia*, "gathering an event defining an action of a first object acting on a target, wherein the first object is executed on a device," "generating contextual state information for the event by correlating the event to an originating object of the first object," "obtaining a global perspective for the event based on the contextual state information, wherein the global perspective comprises information associated with one or more of the first object and the originating object, and wherein the global perspective relates to one or more other events related to the event across a network," "generating an event line comprising information relating to the event, wherein the information relates to at least one of the first object, the action of the first object, the target, and

the originating object," and "transmitting the generated event line." Such limitations cannot be said to merely "calculate[e], and generat[e]." Office Action, pg. 3.

Even if it is assumed, *arguendo*, that the claims are directed to an abstract idea (which Applicant disputes), Applicant respectfully submits that the instant claims recite significantly more than the alleged abstract idea and are therefore still patent eligible. Here, rather than merely reciting instructions to implement the abstract idea on a computer and "implementing these features on a 'memory' or 'processor'" (as was alleged by the Office Action, pg. 3), the claims in fact recite "details regarding how a computer aids the method, the extent to which the computer aids the method, or the significance of a computer to the performance of the method." MPEP § 2106.05(a)(II). Further, the claimed solution could not be construed as "merely adding generic computer components" to perform a well-known or conventional method, as aspects of the claimed solution are specifically rooted in technology. Indeed, as discussed above, the instant claims relate to a specific improvement in computer functionality relating to computer security, and more specifically to providing end-to-end visibility of events within a system and/or network.

The Office Action only generally defines the abstract idea to be "calculating, and generating," and subsequently identifies the additional elements to be "a device, a communication interface, a processor, data storage." Office Action, pg. 3. However, the claims recite specific details in addition to the identified language and do not merely add the words "apply it" or comprise mere instructions to implement the alleged abstract idea on a computer. Indeed, the Office Action omits the majority of the claim language in the above overgeneralization of the claimed subject matter. Further, to the extent that the Office Action is stating that all of the claimed elements for each of the fifteen rejected claims, when considered both individually and as a combination, are well-understood, routine, and convention activities (*see* Office Action, pgs. 3-4, stating that "generic computers performing generic computer functions, alone, do not amount to significantly more than the abstract idea" and that "viewing the elements as a combination does not add anything further than the individual elements"), Applicant respectfully disagrees.

Applicant respectfully requests that the Examiner provide evidence regarding the asserted conventionality as required by the USPTO memo issued on April 19, 2018, titled "Changes in Examination Procedure Pertaining to Subject Matter Eligibility, Recent Subject Matter Eligibility Decision (*Berkheimer v. HP, Inc.*)" (hereinafter the "*Berkheimer* Memo"). As explained in the *Berkheimer* Memo, the Federal Circuit has held in a recent precedential decision that "[w]hether something is well-understood, routine, and conventional to a skilled artisan at the time of the patent is a factual determination." *Berkheimer* Memo, at 2. The *Berkheimer* Memo states that "an examiner should conclude that an element (or combination of elements) represents well-understood, routine, conventional activity **only** when the examiner can readily conclude that the element(s) is widely prevalent or in common use in the relevant industry." *Id.* at 3 (emphasis in original). In addition, any such finding by an examiner must be must be based upon a factual determination supported by evidence. *Id.* at 3. Importantly, "[w]hether a particular technology is well-understood, routine, and conventional goes beyond what was simply known in the prior art. The mere fact that something is disclosed in a piece of prior art, for example, does not mean it was well-understood, routine, and conventional." *Id.* at 3.

In fact, *Berkheimer* has been cited in recent PTAB decisions reversing insufficiently detailed rejections under 35 U.S.C. § 101. For instance, in *Ex parte Bhogal*, the PTAB began by analyzing Step 2B of the § 101 rejection to determine whether "Examiner has proffered sufficient evidence and argument persuading us that claim 1 merely recites conventional computer functions." *Ex parte Bhogal*, Appeal 2016-008742, at 5 (PTAB Mar. 19, 2018). In its analysis, the PTAB cites BASCOM for the premise that "inventive concept can be found in the nonconventional and non-generic arrangement of known, conventional pieces," and subsequently concludes that "the Examiner **has not set forth with sufficient specificity or provided any finding** . . . that the specifically claimed manner of rendering order prioritization technique **is well-understood, routine, or conventional**." *Ex parte Bhogal*, at 6 (emphasis added). In *Ex parte Galloway*, the PTAB similarly concludes that "the Examiner **has not established with appropriate factual evidence** that the claimed method uses conventional cell counting methods," citing again to *Berkheimer*. *Ex parte Galloway*, Appeal 2017-004696, at 9 (PTAB May 24, 2018) (emphasis added).

Here, the claim limitations are not merely conventional or generic, and no appropriate factual evidence has been set forth with sufficient specificity to conclude otherwise. Further, "[w]hether a particular technology is well-understood, routine, and conventional goes beyond what was simply known in the prior art. The mere fact that something is disclosed in a piece of prior art, for example, does not mean it was well-understood, routine, and conventional." *Berkheimer* Memo, at 3. Indeed, "a showing that additional elements are obvious under 35 U.S.C. § 103, or even that they lack novelty under 35 U.S.C. § 102, is not by itself sufficient to establish that the additional elements are well-understood, routine, conventional activities or elements to those in the relevant field." *Berkheimer* Memo, at 3.

Further, in the *Ex parte Blaho* decision from the PTAB (Appeal No. 2016-007954 (Oct. 2, 2017)), the PTAB highlights that the lack of any § 102 or § 103 rejections further weighs in favor of a finding of patentability. The PTAB stated that "[w]e agree that '[t]he Examiner's assertion that the claim elements are routine or conventional is belied by his inability to formulate a rejection under 35 U.S.C. §§ 102 or 103 any longer despite having already cited eight references relevant to remote gaming and having mentioned a number of commercial gaming systems in his rejection under 35 U.S.C. § 101.'" The PTAB further stated, "[i]n essence the Examiner has cited patentable subject matter against the claims at issue and once Appellant demonstrated some patentability over that subject matter, the Examiner now contends that the subject matter relates to unpatentable subject matter. We find such a contention incongruous with the prosecution history of this case."

The present case is similar to the *Ex parte Blaho* case discussed above, in that the obviousness rejections of the claims have all been overcome, leaving only a rejection under § 101. As such, based on the reasoning in *Blaho*, the assertion that the claim elements are merely directed toward generic computers performing generic computer functions is contrary to the lack of any rejections under 35 U.S.C. §§ 102 or 103. Rather, the present claims recite specific limitations that improve the underlying technology in an unconventional manner that does not "monopolize 'the basic tools of scientific and technological work.'" *See Planet Blue*, 837 F.3d at 1314-15.

For at least the reasons set forth above, Applicant respectfully submits the claims recite patent-eligible subject matter and are not directed to an abstract idea. Accordingly, Applicant requests the Examiner to withdraw the § 101 rejection of claims 1-4, 7-11, 13, and 16-20 and issue a Notice of Allowance at the Examiner's earliest convenience.

CONCLUSION

This Response fully responds to the Office Action mailed on May 29, 2018. Still, that Office Action may contain arguments and rejections that are not directly addressed by this Response due to the fact that they are rendered moot in light of the preceding arguments in favor of patentability. Hence, the failure, if any, of this Response to directly address an argument and/or comment raised in the Office Action should not be taken as an indication that the Applicant believes the argument and/or comment has merit. Additionally, the failure, if any, to address statements and/or comments made in the Office Action does not mean that the Applicant acquiesces to such statements and/or comments. Furthermore, the claims of the present application may include other elements, not discussed in this Response, which are not shown, taught, or otherwise suggested by the art of record. Accordingly, the preceding arguments in favor of patentability are advanced without prejudice to other bases of patentability.

It is believed that no further fees are due with this Response. However, the Commissioner is hereby authorized to charge any deficiencies or credit any overpayment with respect to this patent application to deposit account number 13-2725.

In light of the above remarks, it is believed that the application is now in condition for allowance and such action is respectfully requested. Should any additional issues need to be resolved, the Examiner is requested to telephone the undersigned to attempt to resolve those issues.

Respectfully submitted,

Date: August 29, 2018

/Ethan W. Bell/

Ethan W. Bell, Reg. No. 75,549
Merchant & Gould P.C.
P.O. Box 2903
Minneapolis, MN 55402-0903
(303) 357-1211

27488
PATENT TRADEMARK OFFICE

Electronic Acknowledgement Receipt

EFS ID:	33575981
Application Number:	15437275
International Application Number:	
Confirmation Number:	4847
Title of Invention:	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS
First Named Inventor/Applicant Name:	Joseph Jaroch
Customer Number:	23552
Filer:	Ethan Wendel Bell/Julie Borrego
Filer Authorized By:	Ethan Wendel Bell
Attorney Docket Number:	04584.0021USC1
Receipt Date:	29-AUG-2018
Filing Date:	20-FEB-2017
Time Stamp:	15:28:00
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		2018-08_29_RESP_NFOA_04584_0021USC1.pdf	170421 8479b33a5f78d63a8829950c71dbb3b39bee839d	yes	19

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Claims	2	8
	Applicant Arguments/Remarks Made in an Amendment	9	19
Warnings:			
Information:			
	Total Files Size (in bytes):	170421	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

23552 7590 12/26/2018
MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

EXAMINER
SHEHNI, GHAZAL B

ART UNIT	PAPER NUMBER
2436	

DATE MAILED: 12/26/2018

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/437,275	02/20/2017	Joseph Jaroch	04584.0021USC1	4847

TITLE OF INVENTION: METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$1000	$0.00	$0.00	$1000	03/26/2019

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

23552 7590 12/26/2018

MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/437,275	02/20/2017	Joseph Jaroch	04584.0021USC1	4847

TITLE OF INVENTION: METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$1000	$0.00	$0.00	$1000	03/26/2019

EXAMINER	ART UNIT	CLASS-SUBCLASS
SHEHNI, GHAZAL B	2436	726-023000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-09 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. Fees submitted: ❑ Issue Fee ❑ Publication Fee (if required) ❑ Advance Order - # of Copies _____

4b. Method of Payment: *(Please first reapply any previously paid fee shown above)*

❑ Electronic Payment via EFS-Web ❑ Enclosed check ❑ Non-electronic payment by credit card (Attach form PTO-2038)

❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. _____

5. **Change in Entity Status** (from status indicated above)

❑ Applicant certifying micro entity status. See 37 CFR 1.29

❑ Applicant asserting small entity status. See 37 CFR 1.27

❑ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/437,275	02/20/2017	Joseph Jaroch	04584.0021USC1	4847

23552 7590 12/26/2018

MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

EXAMINER	
SHEHNI, GHAZAL B	

ART UNIT	PAPER NUMBER
2436	

DATE MAILED: 12/26/2018

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 15/437,275	Applicant(s) Jaroch et al.	
	Examiner GHAZAL B SHEHNI	Art Unit 2436	AIA Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☑ This communication is responsive to 08/29/2018.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☑ The allowed claim(s) is/are 1-20 . As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see **http://www.uspto.gov/patents/init_events/pph/index.jsp** or send an inquiry to **PPHfeedback@uspto.gov.**

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some *c) ☐ None of the:

   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____ .

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file areply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____ .

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____.
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____.
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date. _____.
5. ☐ Examiner's Amendment/Comment
6. ☐ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/GHAZAL B SHEHNI/
Primary Examiner, Art Unit 2436

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/437,275	Jaroch et al.
	Examiner	Art Unit
	GHAZAL B SHEHNI	2436

CPC - Searched*		
Symbol	Date	Examiner
H04L63/1416 OR H04L63/20 OR H04L63/1425 OR H04L63/1441 OR H04L63/1408 OR H04L63/1433 OR H04L63/145 OR H04L63/14 OR H04L9/3271 OR H04L12/2602	3/28/2017	GS

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
Inventor search (see search history printout)	3/28/2017	GS
East (see search history printout)	3/28/2017	GS
CPC with text search	3/28/2017	GS
East (see search history printout)	11/17/2017	GS
East (see search history printout)	05/23/2018	GS
East (see search history printout)	12/07/2018	GS

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner
726	22, 24, 25	12/07/2018	GS

/GHAZAL B SHEHNI/ Primary Examiner, Art Unit 2436	

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/437,275	Jaroch et al.
	Examiner	**Art Unit**
	GHAZAL B SHEHNI	2436

CPC								
Symbol							**Type**	**Version**
H04L	/	63	/	145			F	2013-01-01
H04L	/	63	/	1416			I	2013-01-01
G06F	/	21	/	56			I	2013-01-01
H04L	/	63	/	1425			I	2013-01-01

CPC Combination Sets									
Symbol							**Type**	**Set**	**Ranking**	**Version**
	/		/							

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	20	
/GHAZAL B SHEHNI/ Primary Examiner, Art Unit 2436	07 December 2018	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	2

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/437,275	Jaroch et al.
	Examiner	**Art Unit**
	GHAZAL B SHEHNI	2436

INTERNATIONAL CLASSIFICATION					
CLAIMED					
G06F	/	21	/	00	
NON-CLAIMED					
	/		/		

US ORIGINAL CLASSIFICATION	
CLASS	**SUBCLASS**
726	23

CROSS REFERENCES(S)						
CLASS	**SUBCLASS (ONE SUBCLASS PER BLOCK)**					
726	22	24	25			

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	20	
/GHAZAL B SHEHNI/ Primary Examiner, Art Unit 2436	07 December 2018	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	2

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/437,275	Jaroch et al.
	Examiner	**Art Unit**
	GHAZAL B SHEHNI	2436

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIMS

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1	11	10	19	19										
2	2	12	11	20	20										
3	3	9	12												
4	4	13	13												
5	5	14	14												
6	6	15	15												
7	7	16	16												
8	8	17	17												
10	9	18	18												

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	20	
/GHAZAL B SHEHNI/ Primary Examiner, Art Unit 2436	07 December 2018	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	2

U.S. Patent and Trademark Office

Part of Paper No.: 20181207

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/437,275	Jaroch et al.
	Examiner	**Art Unit**
	GHAZAL B SHEHNI	2436

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	03/28/2017	11/17/2017	05/23/2018	12/07/2018					
1	1	✓	✓	✓	=					
2	2	✓	✓	✓	=					
3	3	✓	✓	✓	=					
4	4	✓	✓	✓	=					
5	5	✓	✓	O	=					
6	6	✓	✓	O	=					
7	7	✓	✓	✓	=					
8	8	✓	✓	✓	=					
10	9	✓	✓	✓	=					
11	10	✓	✓	✓	=					
12	11	✓	✓	✓	=					
9	12	✓	✓	O	=					
13	13	✓	✓	✓	=					
14	14	✓	✓	O	=					
15	15	✓	✓	O	=					
16	16	✓	✓	✓	=					
17	17	✓	✓	✓	=					
18	18	✓	✓	✓	=					
19	19	✓	✓	✓	=					
20	20	✓	✓	✓	=					

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	10	(("JAROCH") near3 ("Joseph")).INV.	US-PGPUB; USPAT; USOCR	ADJ	ON	2017/03/27 20:14
S2	3	(("ERASMUS") near3 ("Jacques")).INV.	US-PGPUB; USPAT; USOCR	ADJ	ON	2017/03/27 20:14
S3	63	(("BARNES") near3 ("Paul")).INV.	US-PGPUB; USPAT; USOCR	ADJ	ON	2017/03/27 20:14
S4	9	(("MAYR") near3 ("Johannes")).INV.	US-PGPUB; USPAT; USOCR	ADJ	ON	2017/03/27 20:15
S5	2	(("LEIDESDORFF") near3 ("Michael")).INV.	US-PGPUB; USPAT; USOCR	ADJ	ON	2017/03/27 20:15
S6	16	(("GIULIANI") near3 ("Marco")).INV.	US-PGPUB; USPAT; USOCR	ADJ	ON	2017/03/27 20:15
S7	1533	(("WILLIAMS") near3 ("Christopher")).INV.	US-PGPUB; USPAT; USOCR	ADJ	ON	2017/03/27 20:15
S8	2	(("BACHER") near3 ("Chad")).INV.	US-PGPUB; USPAT; USOCR	ADJ	ON	2017/03/27 20:15
S9	880	(virus or malicious or trojan or spy$ware or mal$ware) with ((analyz$3 or analys$3 or determin$5 or detect$4) with (security with event))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/28 14:17
S10	21	(virus or malicious or trojan or spy$ware or mal$ware) with (((analyz$3 or analys$3 or determin$5 or detect$4) with forensic) with (security with (behavior or pattern or event)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/28 14:22
S11	17254	(analys$3 or analyz$3 or detect$4 or monitor$3 or record$3 or captur$3) with ((security with attack) or (network with attack))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/28 14:26
S12	213	(analys$3 or analyz$3 or detect$4 or monitor$3 or record$3 or captur$3) with ((security with attack) or (network with attack)) with forensic	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/28 14:26

S13	111	S12 AND ((H04L63/1416 OR H04L63/20 OR H04L63/1425 OR H04L63/1441 OR H04L63/1408 OR H04L63/1433 OR H04L63/145 OR H04L63/14 OR H04L9/3271 OR H04L12/2602).CPC.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/28 14:29
S14	1	("20130298244").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2017/03/28 14:32
S15	1	("20120260340").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2017/11/17 15:06

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S16	10843	(analysis with forensic)	US-PGPUB; USPAT	ADJ	ON	2017/11/17 14:26
S17	134	(analysis with forensic) with (network with event)	US-PGPUB; USPAT	ADJ	ON	2017/11/17 14:27
S18	6	sniffers with (analysis with forensic)	US-PGPUB; USPAT	ADJ	ON	2017/11/17 14:27
S19	69	(analys$4 or captur$3 or record$3) near7 ((event or computer or file or program or web$page or web$site or site) with network) with security with (sniffer or malicious or virus or trojan or spy$ware)	US-PGPUB; USPAT	ADJ	ON	2017/11/17 14:29
S20	175	(defin$ or analyz$3) with ((behavior or event or computer file or file or program or web$page or web$site) with (network)) with security with (sniffer or malicious or virus or trojan or spy$ware)	US-PGPUB; USPAT	ADJ	ON	2017/11/17 14:48
S21	0	(analys$4 or captur$3 or record$3) near7 (trigger$3 with ((event or computer or file or program or web$page or web$site or site) with network))with security with (sniffer or malicious or virus or trojan or spy$ware)	US-PGPUB; USPAT	ADJ	ON	2017/11/17 14:55
S22	3	(analys$4 or captur$3 or record$3) near7 ((id or identification or identifier) with ((event or computer or file or program or web$page or web$site or site) with network))with security with (sniffer or malicious or virus or trojan or spy$ware)	US-PGPUB; USPAT	ADJ	ON	2017/11/17 14:57
S23	83	(analys$4 or captur$3 or record$3) near7 ((event or computer or file or program or web$page or web$site or site) with network) with security with (sniffer or malicious or virus or trojan or spy$ware)	US-PGPUB; USPAT	ADJ	ON	2018/05/23 17:14
S24	402	(analys$3 or analyz$3 or detect$4 or monitor$3 or record$3 or captur$3) with ((security with attack) or (network with attack)) with forensic	US-PGPUB; USPAT	ADJ	ON	2018/12/06 15:49
S25	24	(analys$4 or captur$3 or record$3) near7 ((event or computer or file or program or web$page or web$site or site) with network)	US-PGPUB; USPAT	ADJ	ON	2018/12/07 17:25

		with security with (sniffer or malicious or virus or trojan or spy$ware) and 726/22-25.ccls.				

12/ 7/ 2018 8:49:46 PM
C:\ Users\ gshehni\ Documents\ EAST\ Workspaces\ 15437275.wsp

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	15437275
Filing Date	2017-02-20
First Named Inventor	Joseph Jaroch
Art Unit	2436
Examiner Name	Shehni, Ghazal B.
Attorney Docket Number	04584.0021USC1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15437275
	Filing Date	2017-02-20
	First Named Inventor	Joseph Jaroch
	Art Unit	2436
	Examiner Name	Shehni, Ghazal B.
	Attorney Docket Number	04584.0021USC1

	1	European Communication in Application 14791882.5, mailed 11/16/2018, 5 pages.	

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	15437275
Filing Date	2017-02-20
First Named Inventor	Joseph Jaroch
Art Unit	2436
Examiner Name	Shehni, Ghazal B.
Attorney Docket Number	04584.0021USC1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☒ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☒ See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Ethan W. Bell/	Date (YYYY-MM-DD)	2019-02-05
Name/Print	Ethan W. Bell	Registration Number	75,549

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal

Application Number:	15437275
Filing Date:	20-Feb-2017
Title of Invention:	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS
First Named Inventor/Applicant Name:	Joseph Jaroch
Filer:	Ethan Wendel Bell/Julie Borrego
Attorney Docket Number:	04584.0021USC1

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
SUBMISSION- INFORMATION DISCLOSURE STMT	1806	1	240	240
		Total in USD ($)		**240**

Electronic Acknowledgement Receipt

EFS ID:	35063340
Application Number:	15437275
International Application Number:	
Confirmation Number:	4847
Title of Invention:	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS
First Named Inventor/Applicant Name:	Joseph Jaroch
Customer Number:	23552
Filer:	Ethan Wendel Bell/Julie Borrego
Filer Authorized By:	Ethan Wendel Bell
Attorney Docket Number:	04584.0021USC1
Receipt Date:	05-FEB-2019
Filing Date:	20-FEB-2017
Time Stamp:	14:53:46
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$240
RAM confirmation Number	020619INTEFSW14542100
Deposit Account	132725
Authorized User	Julie Borrego

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

37 CFR 1.16 (National application filing, search, and examination fees)

37 CFR 1.17 (Patent application and reexamination processing fees)

37 CFR 1.19 (Document supply fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	2019_02_05_2_SIDS_TRANS_LTR_04584_0021USC1.pdf	88185 55c6604f5e0a52d0ccf7647c137599a73116f373	no	2
Warnings:					
Information:					
2	Information Disclosure Statement (IDS) Form (SB08)	2019_02_05_2_SIDS_1449_04584_0021USC1.pdf	611987 c0a4da67a24f23e72520478d4bc59449cf5060ee	no	4
Warnings:					
Information:					
A U.S. Patent Number Citation or a U.S. Publication Number Citation is required in the Information Disclosure Statement (IDS) form for autoloading of data into USPTO systems. You may remove the form to add the required data in order to correct the Informational Message if you are citing U.S. References. If you chose not to include U.S. References, the image of the form will be processed and be made available within the Image File Wrapper (IFW) system. However, no data will be extracted from this form. Any additional data such as Foreign Patent Documents or Non Patent Literature will be manually reviewed and keyed into USPTO systems.					
3	Non Patent Literature	EP_COMM_147918825_11_16_2018_5pgs.PDF	3856857 a2b2d1eb306f8ea48b4e93121e2b0309c42d9b5c	no	5
Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	30798 816195415e48c729bb721ef18912473bbbcb884d	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	4587827		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor:	Joseph Jaroch et al.	Examiner:	Shehni, Ghazal B.
Serial No.:	15/437,275	Group Art Unit:	2436
Filed:	February 20, 2017	Docket No.:	04584.0021USC1
Title:	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS		

Filed via EFS-Web

SECOND SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT (37 C.F.R. § 1.97(d))

Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Attention: Commissioner for Patents

With regard to the above-identified application, the items of information listed on the enclosed Form PTO/SB/08a are brought to the attention of the Examiner.

This statement should be considered because it is submitted after the mailing date of a final action under 37 C.F.R. § 1.113 or after the mailing date of the Notice of Allowance under 37 C.F.R. § 1.311 or after any other action that closes prosecution on the application, but before the payment of the issue fee. Payment is being made via credit card in the amount of $240.00 under 37 C.F.R. § 1.17(p) for consideration of the items listed on the enclosed Form PTO/SB/08a. This statement is submitted as certified below under 37 C.F.R. § 1.97(e)(1) or (2) by the undersigned.

Certification Under 37 C.F.R. § 1.97(e)(1)

In accordance with 37 C.F.R. § 1.97(c) or § 1.97(d), the undersigned hereby certifies that each item of information listed on the enclosed Form PTO/SB/08a was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to filing this statement.

In accordance with 37 C.F.R. § 1.98(a)(2), a copy of each foreign patent and/or a copy of each publication, other than U.S. patents and U.S. patent application publications, listed on the accompanying Form PTO/SB/08a is enclosed.

No representation is made that a reference is "prior art" within the meaning of 35 U.S.C. §§ 102 and 103 and Applicants reserve the right, pursuant to 37 C.F.R. § 1.131 or otherwise, to establish that the reference(s) are not "prior art."

Consideration of the items listed is respectfully requested. Pursuant to the provisions of M.P.E.P. 609, it is requested that the Examiner return a copy of the attached Form PTO/SB/08a, marked as being considered and initialed by the Examiner, to the undersigned with the next official communication.

Please charge any additional fees or credit any overpayment to Deposit Account No. 13-2725.

Respectfully submitted,

Date: February 5, 2019

/Ethan W. Bell/

Ethan W. Bell, Reg. No. 75,549
Merchant & Gould P.C.
P.O. Box 2903
Minneapolis, MN 55402-0903
(303) 357-1211

23552
PATENT TRADEMARK OFFICE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor:	Joseph Jaroch et al.	Examiner:	Shehni, Ghazal B.
Serial No.:	15/437,275	Group Art Unit:	2436
Filed:	February 20, 2017	Docket No.:	04584.0021USC1
Title:	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS		

COMMENTS ON EXAMINER STATEMENT

Commissioner for Patents
P.O. Box 1450
Washington, D.C. 20231

Dear Commissioner:

Applicant acknowledges the allowance of claims 1-20 in the subject application by the Examiner with appreciation. Although the Examiner did not issue a Statement of Reasons for Allowance, Applicant agrees with statements made by the Examiner during the prosecution of the present application to the extent that the claims of the present invention are patentable over the references in the record. However, Applicant does not necessarily acquiesce or agree in any manner as to comments made by the Examiner regarding what the prior art does or does not teach. In addition, Applicant respectfully traverses statements made by the Examiner to the extent that any comment is intended or has the effect of limiting a claim scope, explicitly or implicitly, by not reciting verbatim the respective claim language, or is intended or has the effect of limiting a claim scope by stating or implying that all the reasons for patentability are in any way fully enumerated.

Further reasons for allowance are described and set forth in the Applicant's Specification. As the Examiner's statements are not exhaustive, such statements do not establish an estoppel against Applicant seeking and obtaining allowance of additional, broader claims in a continuation application, which Applicant reserves the right to file.

It is believed that no further fees are due with this Response. However, the Commissioner is hereby authorized to charge any deficiencies or credit any overpayment with respect to this patent application to deposit account number 13-2725.

Respectfully submitted,

Date: February 5, 2019

/Ethan W. Bell/

Ethan W. Bell, Reg. No. 75,549
Merchant & Gould P.C.
P.O. Box 2903
Minneapolis, MN 55402-0903
(303) 357-1211

23552
PATENT TRADEMARK OFFICE

Electronic Patent Application Fee Transmittal

Application Number:	15437275
Filing Date:	20-Feb-2017
Title of Invention:	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS
First Named Inventor/Applicant Name:	Joseph Jaroch
Filer:	Ethan Wendel Bell/Julie Borrego
Attorney Docket Number:	04584.0021USC1

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
UTILITY APPL ISSUE FEE	1501	1	1000	1000

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**1000**

Electronic Acknowledgement Receipt

EFS ID:	35066204
Application Number:	15437275
International Application Number:	
Confirmation Number:	4847
Title of Invention:	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS
First Named Inventor/Applicant Name:	Joseph Jaroch
Customer Number:	23552
Filer:	Ethan Wendel Bell/Julie Borrego
Filer Authorized By:	Ethan Wendel Bell
Attorney Docket Number:	04584.0021USC1
Receipt Date:	05-FEB-2019
Filing Date:	20-FEB-2017
Time Stamp:	16:42:38
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$1000
RAM confirmation Number	020619INTEFSW16431000
Deposit Account	132725
Authorized User	Julie Borrego

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

37 CFR 1.16 (National application filing, search, and examination fees)

37 CFR 1.17 (Patent application and reexamination processing fees)

37 CFR 1.19 (Document supply fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	2019_02_05_ISS_FEE_04584_0021USC1.pdf	91432 249d8e15a52d5fe434bacc1001e49115d2f2b42c	no	1
Warnings:					
Information:					
2	Miscellaneous Incoming Letter	2019_02_05_COMM_ON_EXAM_STMT_04584_0021USC1.pdf	80934 6e3dda57a83f85f2da00666b96017f715c301016	no	2
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30552 bb13145c95220d0d0218c5fc9715cd1f5e97c469	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	202918		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

23552 7590 12/26/2018

MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/437,275	02/20/2017	Joseph Jaroch	04584.0021USC1	4847

TITLE OF INVENTION: METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$1000	$0.00	$0.00	$1000	03/26/2019

EXAMINER	ART UNIT	CLASS-SUBCLASS
SHEHNI, GHAZAL B	2436	726-023000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-09 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____

2 _____

3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: Webroot Inc.

(B) RESIDENCE: (CITY and STATE OR COUNTRY): Broomfield, Colorado

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. Fees submitted: ☒ Issue Fee ☐ Publication Fee (if required) ☐ Advance Order - # of Copies _____

4b. Method of Payment: *(Please first reapply any previously paid fee shown above)*

☒ Electronic Payment via EFS-Web ☐ Enclosed check ☐ Non-electronic payment by credit card (Attach form PTO-2038)

☒ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. 13-2725

5. **Change in Entity Status** (from status indicated above)

☐ Applicant certifying micro entity status. See 37 CFR 1.29

☐ Applicant asserting small entity status. See 37 CFR 1.27

☐ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature /Ethan W. Bell/ Date 2019-02-05

Typed or printed name Ethan W. Bell Registration No. 75,549

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/437,275	02/20/2017	Joseph Jaroch	04584.0021USC1	4847

23552 7590 02/19/2019

MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

EXAMINER	
SHEHNI, GHAZAL B	

ART UNIT	PAPER NUMBER
2436	

NOTIFICATION DATE	DELIVERY MODE
02/19/2019	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

USPTO23552@merchantgould.com

UNITED STATES DEPARTMENT OF COMMERCE
U.S. Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPLICATION NO./ CONTROL NO.	FILING DATE	FIRST NAMED INVENTOR/ PATENT IN REEXAMINATION	ATTORNEY DOCKET NO.
15/437,275	02/20/2017	Jaroch et al.	04584.0021USC1

		EXAMINER	
MERCHANT & GOULD P.C. P.O. BOX 2903 MINNEAPOLIS, MN 55402-0903		GHAZAL B SHEHNI	
		ART UNIT	PAPER
		2436	20190213

DATE MAILED: _____

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner for Patents

Examiner has considered the IDS filed on 02/05/2019.

/GHAZAL B SHEHNI/
Primary Examiner, Art Unit 2436

PTO-90C (Rev.04-03)

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	15437275
Filing Date	2017-02-20
First Named Inventor	Joseph Jaroch
Art Unit	2436
Examiner Name	Shehni, Ghazal B.
Attorney Docket Number	04584.0021USC1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /G.B.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	15437275
Filing Date	2017-02-20
First Named Inventor	Joseph Jaroch
Art Unit	2436
Examiner Name	Shehni, Ghazal B.
Attorney Docket Number	04584.0021USC1

/G.B.S/	1	European Communication in Application 14791882.5, mailed 11/16/2018, 5 pages.	

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/GHAZAL B SHEHNI/	Date Considered	02/13/2019

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /G.B.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	15437275
Filing Date	2017-02-20
First Named Inventor	Joseph Jaroch
Art Unit	2436
Examiner Name	Shehni, Ghazal B.
Attorney Docket Number	04584.0021USC1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☒ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☒ See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Ethan W. Bell/	Date (YYYY-MM-DD)	2019-02-05
Name/Print	Ethan W. Bell	Registration Number	75,549

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /G.B.S/

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /G.B.S/

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/437,275	04/09/2019	10257224	04584.0021USC1	4847

23552 7590 03/20/2019

MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 0 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Joseph Jaroch, Deer Park, IL;
WEBROOT INC., Broomfield, CO;
Jacques Etienne Erasmus, Belper, UNITED KINGDOM;
Paul Barnes, Derby, UNITED KINGDOM;
Johannes Mayr, Linz, AUSTRIA;
Michael Leidesdorff, Niwot, CO;
Marco Giuliani, Bastia Umbra, ITALY;
Christopher Jon Williams, Derbyshire, UNITED KINGDOM;
Chad Edward Bacher, Arvada, CO;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor:	Joseph Jaroch et al.	Examiner:	Shehni, Ghazal B.
Serial No.:	15/437,275	Group Art Unit:	2436
Filed:	February 20, 2017	Docket No.:	04584.0021USC1
Title:	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS		

PETITION UNDER 37 CFR §§ 1.323 & 1.182
AND REQUEST FOR CERTIFICATE OF CORRECTION

Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Dear Commissioner:

Please find a supplemental Application Data Sheet (ADS) attached herewith along with a Certificate of Correction. It was discovered that the original ADS, as filed with the application on February 20, 2017, through error and without deceptive intent, accidentally omitted the middle initial of one of the inventors. Specifically, Joseph **A.** Jaroch's name was listed instead as Joseph Jaroch. In accordance with 35 U.S.C. § 255, the mistake is: (1) of a clerical nature, (2) of a typographical nature, or (3) a mistake of minor character; and the mistake does not involve changes that would (1) constitute new matter or (2) require reexamination. *See* M.P.E.P § 1481. To the extent that a misspelling of an inventor's name does not fall under the provisions of 37 CFR § 1.323 for applicant's mistake, Applicant further petitions for a Certificate of Correction under 37 CFR § 1.182.

It is further requested that a Certificate of Correction be issued correcting printing errors appearing in the above-identified United States patent. Issuance of the Certificate of Correction would not constitute new matter, and re-examination is not required.

Accordingly, Applicant respectfully requests entry of the supplemental ADS and issuance of the Certificate of Correction at the earliest opportunity of the Office. Payment is being made via credit card in the amount of $700.00 under 37 CFR 1.17(f), 37 CFR 1.20(b) and 37 CFR 1.20(a).

Accordingly, it is believed that no further fees are due with this paper. However, the Commissioner is hereby authorized to charge any deficiencies or credit any overpayment with respect to this patent application to deposit account number 13-2725.

Respectfully submitted,

Date: April 12, 2019

/Ethan W. Bell/

Ethan W. Bell, Reg. No. 75,549
Merchant & Gould P.C.
P.O. Box 2903
Minneapolis, MN 55402-0903
(303) 357-1211

23552
PATENT TRADEMARK OFFICE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	04584.0021USC1
	Application Number	15/437,285
Title of Invention	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2:

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Joseph	A.	Jaroch	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Deer Park	State/Province	IL	Country of Residence	US

Mailing Address of Inventor:

Address 1	c/o Webroot Inc.
Address 2	385 Interlocken Crescent, Suite 800

City	Broomfield	State/Province	CO
Postal Code	80021	Country	US

Inventor 2 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Jacques	Etienne	Erasmus	

Residence Information (Select One) ○ US Residency ◉ Non US Residency ○ Active US Military Service

City	Belper	Country of Residence	GB

Mailing Address of Inventor:

Address 1	c/o Webroot Inc.
Address 2	385 Interlocken Crescent, Suite 800

City	Broomfield	State/Province	CO
Postal Code	80021	Country	US

Inventor 3 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Paul		Barnes	

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	04584.0021USC1
	Application Number	15/437,285
Title of Invention	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS	

Residence Information (Select One) ○ US Residency ◉ Non US Residency ○ Active US Military Service

City	Derby	Country of Residence	GB

Mailing Address of Inventor:

Address 1	c/o Webroot Inc.		
Address 2	385 Interlocken Crescent, Suite 800		
City	Broomfield	State/Province	CO
Postal Code	80021	Country	US

Inventor 4 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Johannes		Mayr	

Residence Information (Select One) ○ US Residency ◉ Non US Residency ○ Active US Military Service

City	Linz	Country of Residence	AT

Mailing Address of Inventor:

Address 1	c/o Webroot Inc.		
Address 2	385 Interlocken Crescent, Suite 800		
City	Broomfield	State/Province	CO
Postal Code	80021	Country	US

Inventor 5 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Michael		Leidesdorff	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Niwot	State/Province	CO	Country of Residence	US

Mailing Address of Inventor:

Address 1	c/o Webroot Inc.		
Address 2	385 Interlocken Crescent, Suite 800		
City	Broomfield	State/Province	CO
Postal Code	80021	Country	US

Inventor 6 Remove

Legal Name

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	04584.0021USC1
	Application Number	15/437,285
Title of Invention	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS	

Prefix	Given Name	Middle Name	Family Name	Suffix
	Marco		Giuliani	

Residence Information (Select One) ○ US Residency ◉ Non US Residency ○ Active US Military Service

City	Bastia Umbra	Country of Residence	IT

Mailing Address of Inventor:

Address 1	c/o Webroot Inc.		
Address 2	385 Interlocken Crescent, Suite 800		
City	Broomfield	**State/Province**	CO
Postal Code	80021	**Country**	US

Inventor 7 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Christopher	Jon	Williams	

Residence Information (Select One) ○ US Residency ◉ Non US Residency ○ Active US Military Service

City	Derbyshire	Country of Residence	GB

Mailing Address of Inventor:

Address 1	c/o Webroot Inc.		
Address 2	385 Interlocken Crescent, Suite 800		
City	Broomfield	**State/Province**	CO
Postal Code	80021	**Country**	US

Inventor 8 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Chad	Edward	Bacher	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Arvada	State/Province	CO	Country of Residence	US

Mailing Address of Inventor:

Address 1	c/o Webroot Inc.		
Address 2	385 Interlocken Crescent, Suite 800		
City	Broomfield	**State/Province**	CO
Postal Code	80021	**Country**	US

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	04584.0021USC1
	Application Number	15/437,285
Title of Invention	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS	

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence Information of this application.**

Customer Number	23552		
Email Address	DOCKMPLS@merchantgould.com	Add Email	Remove Email

Application Information:

Title of the Invention	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS		
Attorney Docket Number	04584.0021USC1	**Small Entity Status Claimed**	☐
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	15	**Suggested Figure for Publication (if any)**	2

Filing By Reference:

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	04584.0021USC1
	Application Number	15/437,285
Title of Invention	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS	

Please Select One:	(•) Customer Number	( ) US Patent Practitioner	( ) Limited Recognition (37 CFR 11.9)
Customer Number	23552		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, 365(c), or 386(c) or indicate National Stage entry from a PCT application. Providing benefit claim information in the Application Data Sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.
When referring to the current application, please leave the "Application Number" field blank.

Prior Application Status	~~Pending~~ Patented	Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
15437275	Continuation of	14270069	2014-05-05	9578045	2017-02-21

Prior Application Status	Expired	Remove

Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
14/270069	Claims benefit of provisional	61/819470	2013-05-03

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button.

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55. When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX)[i] the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(i)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

Remove

Application Number	Country[i]	Filing Date (YYYY-MM-DD)	Access Code[i] (if applicable)

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button.

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	04584.0021USC1
	Application Number	15/437,285
Title of Invention	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS	

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	04584.0021USC1
	Application Number	15/437,285
Title of Invention	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS	

Authorization or Opt-Out of Authorization to Permit Access:

When this Application Data Sheet is properly signed and filed with the application, applicant has provided written authority to permit a participating foreign intellectual property (IP) office access to the instant application-as-filed (see paragraph A in subsection 1 below) and the European Patent Office (EPO) access to any search results from the instant application (see paragraph B in subsection 1 below).

Should applicant choose not to provide an authorization identified in subsection 1 below, applicant **must opt-out** of the authorization by checking the corresponding box A or B or both in subsection 2 below.

NOTE: This section of the Application Data Sheet is **ONLY** reviewed and processed with the **INITIAL** filing of an application. After the initial filing of an application, an Application Data Sheet cannot be used to provide or rescind authorization for access by a foreign IP office(s). Instead, Form PTO/SB/39 or PTO/SB/69 must be used as appropriate.

1. Authorization to Permit Access by a Foreign Intellectual Property Office(s)

A. Priority Document Exchange (PDX) - Unless box A in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the State Intellectual Property Office of the People's Republic of China (SIPO), the World Intellectual Property Organization (WIPO), and any other foreign intellectual property office participating with the USPTO in a bilateral or multilateral priority document exchange agreement in which a foreign application claiming priority to the instant patent application is filed, access to: (1) the instant patent application-as-filed and its related bibliographic data, (2) any foreign or domestic application to which priority or benefit is claimed by the instant application and its related bibliographic data, and (3) the date of filing of this Authorization. See 37 CFR 1.14(h)(1).

B. Search Results from U.S. Application to EPO - Unless box B in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the EPO access to the bibliographic data and search results from the instant patent application when a European patent application claiming priority to the instant patent application is filed. See 37 CFR 1.14(h)(2).

The applicant is reminded that the EPO's Rule 141(1) EPC (European Patent Convention) requires applicants to submit a copy of search results from the instant application without delay in a European patent application that claims priority to the instant application.

2. Opt-Out of Authorizations to Permit Access by a Foreign Intellectual Property Office(s)

☐ A. Applicant **DOES NOT** authorize the USPTO to permit a participating foreign IP office access to the instant application-as-filed. If this box is checked, the USPTO will not be providing a participating foreign IP office with any documents and information identified in subsection 1A above.

☐ B. Applicant **DOES NOT** authorize the USPTO to transmit to the EPO any search results from the instant patent application. If this box is checked, the USPTO will not be providing the EPO with search results from the instant application.

NOTE: Once the application has published or is otherwise publicly available, the USPTO may provide access to the application in accordance with 37 CFR 1.14.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	04584.0021USC1
	Application Number	15/437,285
Title of Invention	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS	

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Applicant 1

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

◉ Assignee	○ Legal Representative under 35 U.S.C. 117	○ Joint Inventor
○ Person to whom the inventor is obligated to assign.	○ Person who shows sufficient proprietary interest	

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor:

If the Applicant is an Organization check here. ☒

Organization Name	WEBROOT INC.

Mailing Address Information For Applicant:

Address 1	385 Interlocken Crescent		
Address 2	Suite 800		
City	Broomfield	**State/Province**	CO
Country	US	Postal Code	80021
Phone Number		Fax Number	
Email Address			

Additional Applicant Data may be generated within this form by selecting the Add button.

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	04584.0021USC1
	Application Number	15/437,285
Title of Invention	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS	

Assignee 1

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication. An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

If the Assignee or Non-Applicant Assignee is an Organization check here. ☒

Organization Name	WEBROOT INC.

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1	385 Interlocken Crescent		
Address 2	Suite 800		
City	Broomfield	**State/Province**	CO
Country	US	Postal Code	80021
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button.

Signature:

NOTE: This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b). **However, if this Application Data Sheet is submitted with the INITIAL filing of the application and either box A or B is not checked in subsection 2 of the "Authorization or Opt-Out of Authorization to Permit Access" section, then this form must also be signed in accordance with 37 CFR 1.14(c).**

This Application Data Sheet **must** be signed by a patent practitioner if one or more of the applicants is a **juristic entity** (e.g., corporation or association). If the applicant is two or more joint inventors, this form must be signed by a patent practitioner, **all** joint inventors who are the applicant, or one or more joint inventor-applicants who have been given power of attorney (e.g., see USPTO Form PTO/AIA/81) on behalf of **all** joint inventor-applicants.

See 37 CFR 1.4(d) for the manner of making signatures and certifications.

Signature	/Ethan W. Bell/			Date (YYYY-MM-DD)	2019-04-12
First Name	Ethan	Last Name	Bell	Registration Number	75,549

Additional Signature may be generated within this form by selecting the Add button.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	04584.0021USC1
	Application Number	15/437,285
Title of Invention	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS	

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

PTO/SB/44 (09-07)
Approved for use through 01/31/2020. OMB 0651-0033
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.
(Also Form PTO-1050)

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 10,257,224

APPLICATION NO.: 15/437,275

ISSUE DATE : April 9, 2019

INVENTOR(S) : Joseph A. Jaroch, Jacques Etienne Erasmus, Paul Barnes, Johannes Mayr, Michael Leidesdorff, Marco Giuliani, Christopher Jon Williams and Chad Edward Bacher

It is certified that an error appears or errors appear in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

(72) Inventors: Joseph A. Jaroch, Deer Park, IL (US);
Jacques Etienne Erasmus, Belper (GB);
Paul Barnes, Derby (GB);
Johannes Mayr, Linz (AT);
Michael Leidesdorff, Niwot, CO (US);
Marco Giuliani, Bastia Umbra (IT);
Christopher Jon Williams, Derbyshire (GB);
Chad Edward Bacher, Arvada, CO (US)

Column 1, line 9, "patent application Ser. No. 14/270,069, filed May 5, 2014," should be
-- patent application Ser. No. 14/270,069 (now U.S. Patent No. 9,578,045), filed May 5, 2014, --

MAILING ADDRESS OF SENDER (Please do not use Customer Number below):

Merchant & Gould P.C.
P.O. Box 2903
Minneapolis, MN 55402

This collection of information is required by 37 CFR 1.322, 1.323, and 1.324. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1.0 hour to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Attention Certificate of Corrections Branch, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal

Application Number:	15437275
Filing Date:	20-Feb-2017
Title of Invention:	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS
First Named Inventor/Applicant Name:	Joseph Jaroch
Filer:	Ethan Wendel Bell/Julie Borrego
Attorney Docket Number:	04584.0021USC1

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
PETITION FEE- 37 CFR 1.17(F) (GROUP I)	1462	1	400	400
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
CERTIFICATE OF CORRECTION	1811	1	150	150
PROCESSING FEE CORRECTING INVENTORSHIP	1816	1	150	150
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**700**

Electronic Acknowledgement Receipt

EFS ID:	35714696
Application Number:	15437275
International Application Number:	
Confirmation Number:	4847
Title of Invention:	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS
First Named Inventor/Applicant Name:	Joseph Jaroch
Customer Number:	23552
Filer:	Ethan Wendel Bell/Julie Borrego
Filer Authorized By:	Ethan Wendel Bell
Attorney Docket Number:	04584.0021USC1
Receipt Date:	12-APR-2019
Filing Date:	20-FEB-2017
Time Stamp:	15:54:43
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$700
RAM confirmation Number	041519INTEFSW15551100
Deposit Account	132725
Authorized User	Julie Borrego

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

37 CFR 1.16 (National application filing, search, and examination fees)

37 CFR 1.17 (Patent application and reexamination processing fees)

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Petition for review by the Office of Petitions	2019_04_12_323_and_182_04584_0021USC1.pdf	97533 a649fafd3d31d041de99c91f645ceeb9394bd7dc	no	2
Warnings:					
Information:					
2	Application Data Sheet	2019_04_12_SUPP_ADS_04584_0021USC1.pdf	1304364 e1fdc246964b2683888cc8641286c9c8aa95d23a	no	10
Warnings:					
Information:					
This is not an USPTO supplied ADS fillable form					
3	Request for Certificate of Correction	2019_04_12_CERT_OF_CORR_04584_0021USC1.pdf	172765 f7de90db2bc3f991597408970d0e60b9694c36fd	no	2
Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	33931 9b41622221e48576689f4f1cbeb2a96d7b812479	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1608593		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 10,257,224 B2
APPLICATION NO. : 15/437275
DATED : April 9, 2019
INVENTOR(S) : Joseph A. Jaroch et al.

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

On the Title Page

(72) Inventors should read: Joseph A. Jaroch, Deer Park, IL (US);
Jacques Etienne Erasmus, Belper (GB);
Paul Barnes, Derby (GB);
Johannes Mayr, Linz (AT);
Michael Leidesdorff, Niwot, CO (US);
Marco Giuliani, Bastia Umbra (IT);
Christopher Jon Williams, Derbyshire (GB);
Chad Edward Bacher, Arvada, CO (US)

In the Specification

Column 1, Line 9, "patent application Ser. No. 14/270,069, filed May 5, 2014," should be
-- patent application Ser. No. 14/270,069 (now U.S. Patent No. 9,578,045), filed May 5, 2014, --

Signed and Sealed this
Twenty-first Day of May, 2019

Andrei Iancu
Director of the United States Patent and Trademark Office

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
15/437,275	02/20/2017	2436	1600	04584.0021USC1	20	3

CONFIRMATION NO. 4847

CORRECTED FILING RECEIPT

23552
MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

OC000000112022113

Date Mailed: 10/22/2019

Receipt is acknowledged of this non-provisional utility patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF FIRST INVENTOR, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection.

Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a corrected Filing Receipt, including a properly marked-up ADS showing the changes with strike-through for deletions and underlining for additions. If you received a "Notice to File Missing Parts" or other Notice requiring a response for this application, please submit any request for correction to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections provided that the request is grantable.

Inventor(s)

Joseph A. Jaroch, Deer Park, IL;
Jacques Etienne Erasmus, Belper, UNITED KINGDOM;
Paul Barnes, Derby, UNITED KINGDOM;
Johannes Mayr, Linz, AUSTRIA;
Michael Leidesdorff, Niwot, CO;
Marco Giuliani, Bastia Umbra, ITALY;
Christopher Jon Williams, Derbyshire, UNITED KINGDOM;
Chad Edward Bacher, Arvada, CO;

Applicant(s)

WEBROOT INC., Broomfield, CO;

Assignment For Published Patent Application

WEBROOT INC., Broomfield, CO

Power of Attorney: The patent practitioners associated with Customer Number 23552

Domestic Priority data as claimed by applicant

This application is a CON of 14/270,069 05/05/2014 PAT 9578045
which claims benefit of 61/819,470 05/03/2013

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 02/27/2017
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 15/437,275**
Projected Publication Date: Not Applicable
Non-Publication Request: No
Early Publication Request: No
Title

METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS

Preliminary Class

726

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor

community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/437,275	02/20/2017	Joseph A. Jaroch	04584.0021USC1	4847

23552 7590 10/22/2019

MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

EXAMINER	
SHEHNI, GHAZAL B	

ART UNIT	PAPER NUMBER
2436	

NOTIFICATION DATE	DELIVERY MODE
10/22/2019	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

USPTO23552@merchantgould.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

In re Patent No. 10,257,224	:	
Issue Date: April 9, 2019	:	
Application No. 15/437,275	:	ON PETITION
Filed: February 20, 2017	:	
Attorney Docket No. 04584.0021USC1	:	

This is a decision on the petition under 37 CFR 1.182, filed April 12, 2019, to change the name of the inventor(s).

The petition is **GRANTED**.

The patent file is being forwarded to the Certificates of Correction Branch for issuance of the requested Certificate of Correction.

Telephone inquiries concerning this decision may be directed to the Kimberly Inabinet at (571) 272-4618. Inquiries regarding the issuance of a certificate of correction should be directed to the Certificate of Correction Branch at (571) 272-4200.

Telephone inquiries regarding this decision may be directed to Kimberly Inabinet (571) 272-4618.

/KIMBERLY A INABINET/
Paralegal Specialist, OPET

Attachment: Corrected Filing Receipt

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
15/437,275	02/20/2017	2436	1600	04584.0021USC1	20	3

CONFIRMATION NO. 4847

CORRECTED FILING RECEIPT

23552
MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

OC000000112022113

Date Mailed: 10/22/2019

Receipt is acknowledged of this non-provisional utility patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF FIRST INVENTOR, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection.

Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a corrected Filing Receipt, including a properly marked-up ADS showing the changes with strike-through for deletions and underlining for additions. If you received a "Notice to File Missing Parts" or other Notice requiring a response for this application, please submit any request for correction to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections provided that the request is grantable.

Inventor(s)

Joseph A. Jaroch, Deer Park, IL;
Jacques Etienne Erasmus, Belper, UNITED KINGDOM;
Paul Barnes, Derby, UNITED KINGDOM;
Johannes Mayr, Linz, AUSTRIA;
Michael Leidesdorff, Niwot, CO;
Marco Giuliani, Bastia Umbra, ITALY;
Christopher Jon Williams, Derbyshire, UNITED KINGDOM;
Chad Edward Bacher, Arvada, CO;

Applicant(s)

WEBROOT INC., Broomfield, CO;

Assignment For Published Patent Application

WEBROOT INC., Broomfield, CO

Power of Attorney: The patent practitioners associated with Customer Number 23552

Domestic Priority data as claimed by applicant

This application is a CON of 14/270,069 05/05/2014 PAT 9578045
which claims benefit of 61/819,470 05/03/2013

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 02/27/2017
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 15/437,275**
Projected Publication Date: Not Applicable
Non-Publication Request: No
Early Publication Request: No
Title

METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS

Preliminary Class

726

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor

community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

Power of Attorney to Transact Business with the United States Patent and Trademark Office

I hereby revoke all previous Powers of Attorney given in the application(s) identified in the attached Transmittal for Power of Attorney to One or More Registered Practitioners ("Transmittal Form").

I hereby appoint practitioners associated with the following Customer Number associated with Sprinkle IP Law Group, PC :

109422

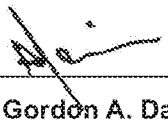
as my/our attorney(s) or agent(s) and to transact all business before the United States Patent and Trademark Office (USPTO) in connection with any and all patents and patent applications that are assigned to **Webroot Inc.** (the "assignee's patents/patent applications") in which they shall appear, any and all assignee's patents/patent applications associated with the above-referenced customer number, and any and all patents and patent applications referenced in the attached Transmittal Form.

Please recognize or change the correspondence address for the patents and patent applications referenced in the attached Transmittal Form to the address associated with the above-referenced customer number.

The undersigned is:

- ☐ Inventor or Joint Inventor
- ☒ Assignee or Person to Whom the Inventor is Under an Obligation to Assign
  *the undersigned has authority to act on behalf of the Assignee or Person to Whom the Inventor is Under an Obligation to Assign.
- ☐ Legal Representative of a Deceased or Legally Incapacitated Inventor
- ☐ Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is currently being filed in this document)

The Transmittal Form may be completed and executed by one of the practitioners associated with the above-referenced customer number.

SIGNATURE OF APPLICANT			
Signature:		**Date:**	January 29, 2020
Name:	**Gordon A. Davies**		
Title:	Director		
Company:	**Webroot Inc.**		
I am authorized to act on behalf of the assignee.			

Electronic Acknowledgement Receipt

EFS ID:	39155610
Application Number:	15437275
International Application Number:	
Confirmation Number:	4847
Title of Invention:	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS
First Named Inventor/Applicant Name:	Joseph A. Jaroch
Customer Number:	23552
Filer:	John L. Adair/keunah cheun
Filer Authorized By:	John L. Adair
Attorney Docket Number:	04584.0021USC1
Receipt Date:	14-APR-2020
Filing Date:	20-FEB-2017
Time Stamp:	15:36:05
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Power of Attorney	WEBROOT_POA_012820.pdf	42303 460c019d47e52952aad549f0d335131a49b6cfef	no	1

Warnings:

Information:	
Total Files Size (in bytes):	42303

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
15/437,275	02/20/2017	Joseph A. Jaroch	04584.0021USC1

CONFIRMATION NO. 4847

POWER OF ATTORNEY NOTICE

23552
MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

OC000000116297636

Date Mailed: 04/21/2020

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 04/14/2020.

- The Power of Attorney to you in this application has been revoked by the assignee who has intervened as provided by 37 CFR 3.71. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/hteffera/

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
15/437,275	02/20/2017	Joseph A. Jaroch	04584.0021USC1

CONFIRMATION NO. 4847

109422
Sprinkle IP Law Group/OPEN
1301 W. 25th Street, Suite 408
Austin, TX 78705

POA ACCEPTANCE LETTER

OC00000016297676

Date Mailed: 04/21/2020

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 04/14/2020.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/hteffera/

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court WESTERN DISTRICT OF TEXAS on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
6:22-cv-00239	3/4/2022	WESTERN DISTRICT OF TEXAS

PLAINTIFF	DEFENDANT
WEBROOT, INC. and OPEN TEXT, INC.	TREND MICRO INC.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	8,418,250	4/9/2013	Webroot, Inc.
2	8,726,389	5/13/2014	Webroot, Inc.
3	9,578,045	2/21/2017	Webroot, Inc.
4	10,257,224	4/9/2019	Webroot, Inc.
5	10,284,591	5/7/2019	Webroot, Inc.

In the above---entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 10,499,844	12/10/2019	Webroot, Inc.
2		
3		
4		
5		

In the above---entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1---Upon initiation of action, mail this copy to Director Copy 3---Upon termination of action, mail this copy to Director
Copy 2---Upon filing document adding patent(s), mail this copy to Director Copy 4---Case file copy

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court WESTERN DISTRICT OF TEXAS on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
6:22-cv-00240	3/4/2022	WESTERN DISTRICT OF TEXAS

PLAINTIFF	DEFENDANT
WEBROOT, INC. and OPEN TEXT, INC.	SOPHOS LTD.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	8,418,250	4/9/2013	Webroot, Inc.
2	8,726,389	5/13/2014	Webroot, Inc.
3	9,578,045	2/21/2017	Webroot, Inc.
4	10,257,224	4/9/2019	Webroot, Inc.
5	10,284,591	5/7/2019	Webroot, Inc.

In the above---entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading		
	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	10,499,844	12/10/2019	Webroot, Inc.
2	9,413,721	8/9/2016	Webroot, Inc.
3			
4			
5			

In the above---entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1---Upon initiation of action, mail this copy to Director Copy 3---Upon termination of action, mail this copy to Director
Copy 2---Upon filing document adding patent(s), mail this copy to Director Copy 4---Case file copy

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court WESTERN DISTRICT OF TEXAS on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
6:22-cv-00241	3/4/2022	WESTERN DISTRICT OF TEXAS

PLAINTIFF	DEFENDANT
WEBROOT, INC. and OPEN TEXT, INC.	CROWDSTRIKE, INC. and CROWDSTRIKE HOLDINGS, INC.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	8,418,250	4/9/2013	Webroot, Inc.
2	8,726,389	5/13/2014	Webroot, Inc.
3	9,578,045	2/21/2017	Webroot, Inc.
4	10,257,224	4/9/2019	Webroot, Inc.
5	10,284,591	5/7/2019	Webroot, Inc.

In the above---entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 10,499,844	12/10/2019	Webroot, Inc.
2		
3		
4		
5		

In the above---entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1---Upon initiation of action, mail this copy to Director Copy 3---Upon termination of action, mail this copy to Director
Copy 2---Upon filing document adding patent(s), mail this copy to Director Copy 4---Case file copy

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court WESTERN DISTRICT OF TEXAS on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
6:22-cv-00243	3/4/2022	WESTERN DISTRICT OF TEXAS

PLAINTIFF	DEFENDANT
WEBROOT, INC. and OPEN TEXT, INC.	AO KASPERSKY LAB

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	8,418,250	4/9/2013	Webroot, Inc.
2	8,726,389	5/13/2014	Webroot, Inc.
3	9,578,045	2/21/2017	Webroot, Inc.
4	10,257,224	4/9/2019	Webroot, Inc.
5	10,284,591	5/7/2019	Webroot, Inc.

In the above---entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 10,499,844	12/10/2019	Webroot, Inc.
2		
3		
4		
5		

In the above---entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1---Upon initiation of action, mail this copy to Director Copy 3---Upon termination of action, mail this copy to Director
Copy 2---Upon filing document adding patent(s), mail this copy to Director Copy 4---Case file copy