

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
---	---

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. 6:22-cv-00243	DATE FILED 3/4/2022	U.S. DISTRICT COURT WESTERN DISTRICT OF TEXAS
PLAINTIFF WEBROOT, INC. and OPEN TEXT, INC.		DEFENDANT 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

Trend Micro, Inc.
EX1006-1

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
---	---

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. 6:22-cv-00241	DATE FILED 3/4/2022	U.S. DISTRICT COURT WESTERN DISTRICT OF TEXAS
PLAINTIFF WEBROOT, INC. and OPEN TEXT, INC.		DEFENDANT 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

Trend Micro, Inc.
EX1006-2

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
---	---

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. 6:22-cv-00240	DATE FILED 3/4/2022	U.S. DISTRICT COURT WESTERN DISTRICT OF TEXAS
PLAINTIFF WEBROOT, INC. and OPEN TEXT, INC.		DEFENDANT 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

Trend Micro, Inc.
EX1006-3

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
---	---

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. 6:22-cv-00239	DATE FILED 3/4/2022	U.S. DISTRICT COURT WESTERN DISTRICT OF TEXAS
PLAINTIFF WEBROOT, INC. and OPEN TEXT, INC.		DEFENDANT 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

Trend Micro, Inc.
EX1006-4



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

POA ACCEPTANCE LETTER

109422
Sprinkle IP Law Group/OPEN
1301 W. 25th Street, Suite 408
Austin, TX 78705



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.

/hteffer/



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



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.

/hteffer/

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	no	1
			460c019d47e52952aad549f0d335131a49b6cfeef		

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. <u>New Applications Under 35 U.S.C. 111</u> 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. <u>National Stage of an International Application under 35 U.S.C. 371</u> 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. <u>New International Application Filed with the USPTO as a Receiving Office</u> 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 A. Jaroch	04584.0021USC1	4847
23552	7590	10/22/2019		
MERCHANT & GOULD P.C.			EXAMINER	
P.O. BOX 2903			SHEHNI, GHAZAL B	
MINNEAPOLIS, MN 55402-0903				
			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



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 Assets Control, 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 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



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 Assets Control, 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
CERTIFICATE OF CORRECTION

PATENT NO. : 10,257,224 B2
APPLICATION NO. : 15/437275
DATED : April 9, 2019
INVENTOR(S) : Joseph A. Jaroch et al.

Page 1 of 1

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

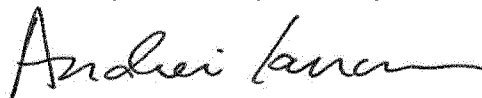
On the Title Page

(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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor:	Joseph Jarocho 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. Jarocho's name was listed instead as Joseph Jarocho. 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



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 Residenceⁱ	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	Countryⁱ	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 Residenceⁱ	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	Countryⁱ	US			
Inventor 3					Remove	
Legal Name						
Prefix	Given Name	Middle Name	Family Name	Suffix		
	Paul		Barnes	Trend Micro, Inc.		

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	04584.0021USC1
		Application Number	<u>15/437,285</u>
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

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		

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	<u>15/437,285</u>
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.

Trend Micro, Inc.

EX1006-26

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	<u>15/437,285</u>
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~~ <u>Patented</u>	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	<u>9578045</u>	<u>2017-02-21</u>
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 ^j (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	<u>15/437,285</u>
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	<u>15/437,285</u>
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	<u>15/437,285</u>
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	
☐ Person to whom the inventor is obligated to assign.		☐ Joint Inventor	
☐ 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	<u>15/437,285</u>
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 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.

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	<u>15/437,285</u>
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.**

**UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION**Page 1 of 1

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.

Trend Micro, Inc.
EX1006-33

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)

Trend Micro, Inc.

EX1006-37

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	no	2
			a649fafd3d31d041de99c91f645ceeb9394bd7dc		
Warnings:					
Information:					
2	Application Data Sheet	2019_04_12_SUPP_ADS_04584_0021USC1.pdf	1304364	no	10
			e1fdc246964b2683888cc8641286c9c8aa95d23a		
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	no	2
			f7de90db2bc3f991597408970d0e60b9694c36fd		
Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	33931	no	2
			9b41622221e48576689f4f1cbeb2a96d7b812479		
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

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.



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	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	Jaroach et al.	04584.0021USC1

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

Doc code: IDS

PTO/SB/08a (01-10)

Doc description: Information Disclosure Statement (IDS) Filed

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 ²ⁱ	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 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.

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 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 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.

S/N 15/437,275

PATENT

CONF. NO. 4847

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.

Application Serial No. 15/437,275
Comments On Statement Of Reasons For Allowance

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

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)

Trend Micro, Inc.

EX1006-51

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	no	1
			249d8e15a52d5fe434bacc1001e49115d2f2b42c		

Warnings:

Information:

2	Miscellaneous Incoming Letter	2019_02_05_COMM_ON_EXAM_STMT_04584_0021USC1.pdf	80934	no	2
			6e3dda57a83f85f2da00666b96017f715c301016		

Warnings:

Information:

3	Fee Worksheet (SB06)	fee-info.pdf	30552	no	2
			bb13145c95220d0d0218c5fc9715cd1f5e97c469		

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)

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.

23552 7590 12/26/2018
MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

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,

1 _____

(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.

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)

Webroot Inc.

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

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 ²ⁱ	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 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 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)

Trend Micro, Inc.

EX1006-60

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_L TR_04584_0021USC1.pdf	88185	no	2
			55c6604f5e0a52d0ccf7647c137599a73116f373		
Warnings:					
Information:					
2	Information Disclosure Statement (IDS) Form (SB08)	2019_02_05_2_SIDS_1449_045 84_0021USC1.pdf	611987	no	4
			c0a4da67a24f23e72520478d4bc59449cf5060ee		
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	no	5
			a2b2d1eb306f8ea48b4e93121e2b0309c42d9b5c		
Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	30798	no	2
			816195415e48c729bb721ef18912473bbcb884d		
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.

S/N 15/437,275

PATENT
CONF. NO. 4847

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





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)

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.

23552 7590 12/26/2018
MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

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,

1 _____

(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.

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	EXAMINER	
MERCHANT & GOULD P.C. P.O. BOX 2903 MINNEAPOLIS, MN 55402-0903			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 a reply 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)	5. ☐ Examiner's Amendment/Comment
2. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____.	6. ☐ Examiner's Statement of Reasons for Allowance
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____.	7. ☐ Other _____.
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date. _____.	

/GHAZAL B SHEHNI/ Primary Examiner, Art Unit 2436	
--	--

Search Notes 	Application/Control No. 15/437,275	Applicant(s)/Patent Under Reexamination Jaroch et al.
	Examiner GHAZAL B SHEHNI	Art Unit 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. 15/437,275	Applicant(s)/Patent Under Reexamination Jaroch et al.
	Examiner GHAZAL B SHEHNI	Art Unit 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
	/		/		

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

<i>Issue Classification</i> 	Application/Control No. 15/437,275	Applicant(s)/Patent Under Reexamination Jaroch et al.
	Examiner GHAZAL B SHEHNI	Art Unit 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. 15/437,275	Applicant(s)/Patent Under Reexamination Jaroch et al.
	Examiner GHAZAL B SHEHNI	Art Unit 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

<i>Index of Claims</i> 	Application/Control No. 15/437,275	Applicant(s)/Patent Under Reexamination Jaroch et al.
	Examiner GHAZAL B SHEHNI	Art Unit 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	((("LEI DESDORFF") 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 (I nterference)

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

S/N 15/437,275

PATENT

Conf. No. 4847

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 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



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	yes	19
			8479b33a5f78d63a8829950c71d0b3b39be e839d		

	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

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.			EXAMINER	
P.O. BOX 2903			SHEHNI, GHAZAL B	
MINNEAPOLIS, MINNESOTA 55402-0903				
UNITED STATES OF AMERICA				
			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

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

Search Notes 	Application/Control No. 15/437,275	Applicant(s)/Patent Under Reexamination Jaroch et al.
	Examiner GHAZAL B SHEHNI	Art Unit 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

PTO/SB/08a (03-15)

Doc description: Information Disclosure Statement (IDS) Filed

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 ²ⁱ	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 JAROCK
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):

☒ 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)	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 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 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.

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	((("LEI DESDORFF") 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 (I nterference)

< This search history is empty>

5/ 23/ 2018 5:16:16 PM
C:\ Users\ gshehni\ Documents\ EAST\ Workspaces\ 15437275.wsp

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									
		(Column 1)	(Column 2)						
FOR		NUMBER FILED	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), (l), 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	
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.

S/N 15/437,275

PATENT

Conf. No. 4847

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

S/N 15/437,275

PATENT

Conf. No. 4847

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

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):

	<u>Fee</u>	<u>Small Entity Fee</u>	<u>Micro Entity Fee</u>	
☐ One month (37 CFR 1.17(a)(1))	\$200	\$100	\$50	\$ _____
☒ Two months (37 CFR 1.17(a)(2))	\$600	\$300	\$150	\$ <u>600</u>
☐ 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)

Trend Micro, Inc.

EX1006-128

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	no	1
			a438583adce29da7d464488fe4a5039bf3645633		

Warnings:

This is not a USPTO supplied RCE SB30 form.

Information:

2		2018_04_23_RESP_AA_04584_0021USC1.pdf	106891	yes	10
			fac5fcaf6c0e840d299c897637fc65245fb2e1b7		

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	no	1
			5c6403c7315fcbbd7ec75c4fbfd36019803875aa		

Warnings:**Information:**

4	Fee Worksheet (SB06)	fee-info.pdf	32917	no	2
			62ec4cef9419c128067102f92102d8935bc68403		

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.



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	EXAMINER	
MERCHANT & GOULD P.C.			SHEHNI, GHAZAL B	
P.O. BOX 2903			ART UNIT	PAPER NUMBER
MINNEAPOLIS, MN 55402-0903			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
--	--

S/N 15/437,275

PATENT

Conf. No. 4847

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)

S/N 15/437,275

PATENT

Conf. No. 4847

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



S/N 15/437,275

PATENT

Conf. No. 4847

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

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 ²ⁱ	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):

☒ 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)	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 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 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)

Trend Micro, Inc.

EX1006-145

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	yes	3
			16d75c1aa8a1692e44ff246e202d3a3d39afe6ca		
	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	no	2
			b016b6627b7cbbe5d7956d7a966f42582025b7b9		
Warnings:					
Information:					
3	Information Disclosure Statement (IDS) Form (SB08)	2018_02_22_SIDS_1449_04584_0021USC1.pdf	1006857	no	4
			ba97157938abba44dd7a4d87029ef71fc7972f92		
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	no	6
			bd7fe579c116376e3106dc46dd214d8673f691c9		
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	no	2
			1bca3d0dd40b56e2d08b0136c3df94b740af8a28		

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 OBIVIATE 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 <u>75549</u> ☐ 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)

Trend Micro, Inc.

EX1006-153

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	no	2
			ac8f582e64ca5e216f414b0f11498efbe042115d		

Warnings:

Information:

2	Fee Worksheet (SB06)	fee-info.pdf	30777	no	2
			a3ea81cb4388acd85c6b32bfdfee5b02591c6a8		

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	11/22/2017	EXAMINER	
MERCHANT & GOULD P.C.			SHEHNI, GHAZAL B	
P.O. BOX 2903			ART UNIT	PAPER NUMBER
MINNEAPOLIS, MN 55402-0903			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) | 3) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) ☒ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b)
Paper No(s)/Mail Date <u>08/21/2017</u> | 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/

Application/Control Number: 15/437,275

Page 6

Art Unit: 2436

Primary Examiner, Art Unit 2436

Doc code: IDS

PTO/SB/08a (03-15)

Doc description: Information Disclosure Statement (IDS) Filed

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.

FOREIGN PATENT DOCUMENTS

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

NON-PATENT LITERATURE DOCUMENTS

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

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 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 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.

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

<i>Index of Claims</i> 	Application/Control No. 15437275	Applicant(s)/Patent Under Reexamination JAROCH ET AL.
	Examiner GHAZAL SHEHNI	Art Unit 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. 15437275	Applicant(s)/Patent Under Reexamination JAROCH ET AL.
	Examiner GHAZAL SHEHNI	Art Unit 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:	Jaroach 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

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 02-20-2017	
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):

	<u>Fee</u>	<u>Small Entity Fee</u>	<u>Micro Entity Fee</u>	
☐ One month (37 CFR 1.17(a)(1))	\$200	\$100	\$50	\$ _____
☒ Two months (37 CFR 1.17(a)(2))	\$600	\$300	\$150	\$ <u>600.00</u>
☐ 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 _____.

<u>/Ethan W. Bell/</u> Signature <u>Ethan W. Bell</u> Typed or printed name	<u>2017-09-05</u> Date <u>303-357-1211</u> 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	yes	15
			0d3ad57efc4928eb75977ea5ed025868785bf13e		
	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	no	2
			8b7631484e82b8213ec6b6f6d7084594d447c46c		
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	31180	no	2
			1ff617fc830eccc518ba0e200c337f26c27ece61		
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.

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										
(Column 1)		(Column 2)								
FOR	NUMBER FILED	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										
(Column 1)		(Column 2)		(Column 3)						
AMENDMENT	09/05/2017	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 \$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			
(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 \$ =				
	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.

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

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 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 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.

(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): **MARK-MONITOR, 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).

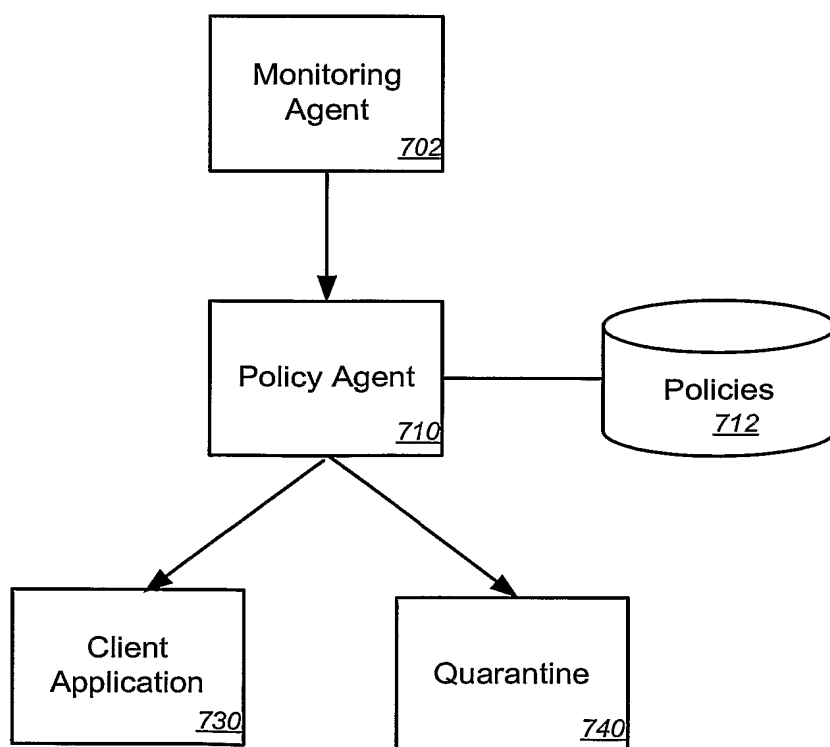
(74) Agents: **KING, Chad** et al.; Townsend and Townsend and Crew LLP, Two Embarcadero Center, Eighth Floor, San Francisco, California 94111-3834 (US).

(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. 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.



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 identify 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 policies 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, policies 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 entities.

[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 reputation) 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 appreciated 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 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 which 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 propagated 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