

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

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

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

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



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
14/270,069	05/05/2014	Joseph Jaroch	04584.0021USU1

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

CONFIRMATION NO. 9580
POWER OF ATTORNEY NOTICE



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/



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
14/270,069	05/05/2014	Joseph Jaroch	04584.0021USU1

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

CONFIRMATION NO. 9580
POA ACCEPTANCE LETTER



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/

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:	39155018
Application Number:	14270069
International Application Number:	
Confirmation Number:	9580
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:	John L. Adair/keunah cheun
Filer Authorized By:	John L. Adair
Attorney Docket Number:	04584.0021USU1
Receipt Date:	14-APR-2020
Filing Date:	05-MAY-2014
Time Stamp:	15:11:47
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
			460c019d47e52952aad549f0d335131a49b6cfe		

Warnings:

IPR2023-00126

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.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/270,069	02/21/2017	9578045	04584.0021USU1	9580

23552 7590 02/01/2017
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 (PG), 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.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: **Mail** **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax **(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 10/05/2016
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 facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/270,069	05/05/2014	Joseph Jaroch	04584.0021USU1	9580

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	\$960	\$0	\$0	\$960	01/05/2017

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 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

- (1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
- (2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 Merchant & Gould P.C.

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 has been filed for recordation as set forth in 37 CFR 3.11. 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. The following fee(s) are submitted:

- ☒ Issue Fee
- ☐ Publication Fee (No small entity discount permitted)
- ☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): (Please first reapply any previously paid issue fee shown above)

- ☐ A check is enclosed.
- ☒ Payment by credit card. Form PTO-2038 is attached.
- ☒ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number 132725 (enclose an extra copy of this form).

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 /Andrew T. Pouzeshi/

Date January 5, 2017

Typed or printed name Andrew T. Pouzeshi

Registration No. 67672

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Jaroach et al.	Examiner:	Shehni, Ghazal B.
Serial No.:	14/270,069	Group Art Unit:	2436
Filed:	May 5, 2014	Docket No.:	04584.0021USU1
Title:	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS		

COMMENTS ON EXAMINER STATEMENT

Mail Stop – ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Washington, D.C. 20231

Dear Commissioner:

Applicant acknowledges the allowance of claims 1-7 and 9-20 in the subject application by the Examiner with appreciation. Although the Examiner did not issue a Statement of Reasons for Allowance, Applicant agrees with statements made by the Examiner during the prosecution of the present application to the extent that the claims of the present invention are patentable over the references in the record. However, Applicant does not necessarily acquiesce or agree in any manner as to comments made by the Examiner regarding what the prior art does or does not teach. In addition, Applicant respectfully traverses statements made by the Examiner to the extent that any comment is intended or has the effect of limiting a claim scope, explicitly or implicitly, by not reciting verbatim the respective claim language, or is intended or has the effect of limiting a claim scope by stating or implying that all the reasons for patentability are in any way fully enumerated.

Further reasons for allowance are described and set forth in the Applicant's Specification. As the Examiner's statements are not exhaustive, such statements do not establish an estoppel against Applicant seeking and obtaining allowance of additional, broader claims in a continuation application, which Applicant reserves the right to file.

It is believed that no further fees are due with this Response. However, the Commissioner is hereby authorized to charge any deficiencies or credit any overpayment with respect to this patent application to deposit account number 13-2725.

Respectfully submitted,

Date: January 5, 2017



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

Electronic Patent Application Fee Transmittal

Application Number:	14270069			
Filing Date:	05-May-2014			
Title of Invention:	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS			
First Named Inventor/Applicant Name:	Joseph Jaroch			
Filer:	Andrew T. Pouzeshi/Jacquelyn Slate			
Attorney Docket Number:	04584.0021USU1			
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	960	960

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				960

Electronic Acknowledgement Receipt

EFS ID:	27982225
Application Number:	14270069
International Application Number:	
Confirmation Number:	9580
Title of Invention:	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS
First Named Inventor/Applicant Name:	Joseph Jaroch
Customer Number:	23552
Filer:	Andrew T. Pouzeshi/Jacquelyn Slate
Filer Authorized By:	Andrew T. Pouzeshi
Attorney Docket Number:	04584.0021USU1
Receipt Date:	05-JAN-2017
Filing Date:	05-MAY-2014
Time Stamp:	15:40:44
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	\$960
RAM confirmation Number	010617INTEFSW15415500
Deposit Account	
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

IPR2023-00126

CrowdStrike EX1010 Page 16

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)	2017-01-05- IssueFeeTrans-04584-0021USU 1.PDF	1101500 85ac7a47fb661efa93ae5307ffc447248351 767	no	1
Warnings:					
Information:					
2	Post Allowance Communication - Incoming	2017-01-05- Comments-04584-0021USU1. PDF	70927 3a6b162f081a5d3a48199c552a993b1ce7d b1336	no	2
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	31078 20af807688245aa8e54e2bed0e782d305fc5 f99c	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			1203505		
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

NOTICE OF ALLOWANCE AND FEE(S) DUE

23552 7590 10/05/2016
MERCHANT & GOULD P.C.
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

EXAMINER

SHEHNI, GHAZAL B

ART UNIT

PAPER NUMBER

2436

DATE MAILED: 10/05/2016

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

14/270,069

05/05/2014

Joseph Jaroch

04584.0021USU1

9580

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	\$960	\$0	\$0	\$960	01/05/2017

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: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: **Mail** **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (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 10/05/2016
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 facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/270,069	05/05/2014	Joseph Jaroch	04584.0021USU1	9580

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	\$960	\$0	\$0	\$960	01/05/2017

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 03-02 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 has been filed for recordation as set forth in 37 CFR 3.11. 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. The following fee(s) are submitted:

- ☐ Issue Fee
- ☐ Publication Fee (No small entity discount permitted)
- ☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): (Please first reapply any previously paid issue fee shown above)

- ☐ A check is enclosed.
- ☐ Payment by credit card. Form PTO-2038 is attached.
- ☐ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

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.
14/270,069	05/05/2014	Joseph Jaroch	04584.0021USU1	9580

23552	7590	10/05/2016
MERCHANT & GOULD P.C.		
P.O. BOX 2903		
MINNEAPOLIS, MN 55402-0903		

EXAMINER
SHEHNI, GHAZAL B

ART UNIT	PAPER NUMBER
2436	

DATE MAILED: 10/05/2016

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 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, 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.

Notice of Allowability	Application No. 14/270,069	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--

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 08/31/2016.
☐ 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 1-7 and 9-20. 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 SHEHNI/
Primary Examiner, Art Unit 2436

DETAILED ACTION

Claims 1-7, 9-20 are allowed.

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in telephonic interview from Mr. Andrew T. Pouzeshi on September 22, 2016.

The application has been amended as follows:

Amend the following **claim 12**.

12. The system of claim ~~8~~ 9, wherein the sensor agent is further operable to: cache the one or more events; and asynchronously consolidate and normalize the one or more events.

Art Unit: 2436

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

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.

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.

Application/Control Number: 14/270,069
Art Unit: 2436

Page 4

/GHAZAL SHEHNI/
Primary Examiner, Art Unit 2436

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	113	(network with event) with (analysis with forensic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2016/09/22 16:07
L2	42	1 AND ((G06F21/52 OR G06F17/30628 OR G06F21/552 OR G06F17/30002 OR G06F21/56 OR G06F21/577 OR G06F2009/45587 OR G06F2009/45591).CPC.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2016/09/22 16:08
S27	16	(analy\$4 or captur\$3 or record\$3) near7 (event with (network)) with security with (sniffer or malicious or virus or trojan or spy\$ware)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2016/09/21 20:35
S28	86	(network with forensic) with sniffers	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2016/09/21 20:35
S29	113	(network with event) with (analysis with forensic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2016/09/21 20:35
S30	1	("20140115159").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2016/09/22 13:12

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S31	4430	(network or internet or electronic) with (forensic or evidence or malicious) with (analysis or analyz\$5 or determin\$7)	US-PGPUB; USPAT	ADJ	ON	2016/09/21 21:31
S32	13	(network or internet or electronic) with (forensic or evidence or malicious) with (analysis or analyz\$5 or determin\$7) near7 (event with (network)) with security with (sniffer or malicious or virus or trojan or spy\$ware)	US-PGPUB; USPAT	ADJ	ON	2016/09/21 21:32
S33	12	(analy\$4 or captur\$3 or record\$3) near7 (event with (network)) with security with (sniffer or malicious or virus or trojan or spy\$ware)	US-PGPUB; USPAT	ADJ	ON	2016/09/21 21:52
S34	3	(analy\$4 or captur\$3 or record\$3) near7 ((event or computer file or file or program or web\$page web\$site) with (network)) with security with (sniffer or malicious or virus or trojan or spy\$ware).clm.	US-PGPUB; USPAT	ADJ	ON	2016/09/21 22:02

S35	43	(defin\$3 or analyz\$3) with ((behavior or event or computer file or file or program or web\$page web\$site) with (network)) with security with (sniffer or malicious or virus or trojan or spy\$ware) and 726/22-25.ccls.	US-PGPUB; USPAT	ADJ	ON	2016/09/21 22:06
-----	----	--	-----------------	-----	----	------------------

9/ 22/ 2016 4:13:28 PM
C:\ Users\ gshehni\ Documents\ EAST\ Workspaces\ 14270069.wsp

Search Notes 	Application/Control No. 14270069	Applicant(s)/Patent Under Reexamination JAROCH ET AL.
	Examiner GHAZAL SHEHNI	Art Unit 2436

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner
G06F21/52 OR G06F17/30628 OR G06F21/552 OR G06F17/30002 OR G06F21/56 OR G06F21/577 OR G06F2009/45587 OR G06F2009/45591	9/22/2016	GS

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
726	All	9/2/2015	GS

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor search (see search history printout)	9/2/2015	GS
East (see search history printout)	9/2/2015	GS
class 726 with text search	9/2/2015	GS
East (see search history printout)	5/24/2016	GS
East (see search history printout)	9/22/2016	GS

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
726	22, 24-25	9/22/2016	GS

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

<i>Index of Claims</i> 	Application/Control No. 14270069	Applicant(s)/Patent Under Reexamination JAROCK 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	09/02/2015	05/24/2016	09/22/2016															
1	1	✓	✓	=															
2	2	✓	✓	=															
3	3	✓	✓	=															
4	4	✓	✓	=															
5	5	✓	✓	=															
6	6	✓	✓	=															
7	7	✓	✓	=															
-	8	✓	-	-															
8	9	✓	✓	=															
9	10	✓	✓	=															
10	11	✓	✓	=															
11	12	✓	✓	=															
12	13	✓	✓	=															
13	14	✓	✓	=															
14	15	✓	✓	=															
15	16	✓	✓	=															
16	17	✓	✓	=															
17	18	✓	✓	=															
18	19	✓	✓	=															
19	20	O	O	=															

Issue Classification 	Application/Control No. 14270069	Applicant(s)/Patent Under Reexamination JAROCH ET AL.
	Examiner GHAZAL SHEHNI	Art Unit 2436

CPC						
Symbol					Type	Version
H04L		63	/	1416	F	2013-01-01
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			

CPC Combination Sets				
Symbol	Type	Set	Ranking	Version
				
				

NONE	Total Claims Allowed: 19	
(Assistant Examiner)	(Date)	
/GHAZAL SHEHNI/ Primary Examiner.Art Unit 2436	09/22/2016	O.G. Print Claim(s) 1
(Primary Examiner)	(Date)	O.G. Print Figure 2

Issue Classification 	Application/Control No. 14270069	Applicant(s)/Patent Under Reexamination JAROCH ET AL.
	Examiner GHAZAL SHEHNI	Art Unit 2436

☐ Claims renumbered in the same order as presented by applicant															
☐ CPA															
☐ T.D.															
☐ R.1.47															
Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1	16	17												
2	2	17	18												
3	3	18	19												
4	4	19	20												
5	5														
6	6														
7	7														
-	8														
8	9														
9	10														
10	11														
11	12														
12	13														
13	14														
14	15														
15	16														

NONE	Total Claims Allowed: 19	
(Assistant Examiner)	(Date)	
/GHAZAL SHEHNI/ Primary Examiner.Art Unit 2436	09/22/2016	O.G. Print Claim(s) 1
(Primary Examiner)	(Date)	O.G. Print Figure 2

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 14/270,069	Filing Date 05/05/2014	☐ 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 \$ =	
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	03/16/2016	CLAIMS REMAINING AFTER AMENDMENT	MINUS	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)
	Total (37 CFR 1.16(i))	* 19	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	08/31/2016	CLAIMS REMAINING AFTER AMENDMENT	MINUS	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)
	Total (37 CFR 1.16(i))	* 19	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

* 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
JEFFERY L. OLSEN

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.

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL **(Submitted Only via EFS-Web)**

Application Number	14270069	Filing Date	2014-05-05	Docket Number (if applicable)	04584.0021USU1	Art Unit	2436
First Named Inventor	Joseph Jaroch			Examiner Name	SHEHNI, GHAZAL B.		

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.

Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV

SUBMISSION REQUIRED UNDER 37 CFR 1.114

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____

☐ Other _____

☒ Enclosed

☒ Amendment/Reply

☐ Information Disclosure Statement (IDS)

☐ Affidavit(s)/ Declaration(s)

☐ Other _____

MISCELLANEOUS

☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months _____
 (Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

☐ Other _____

FEES

☒ The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.
 The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to
 Deposit Account No 132725

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

☒ Patent Practitioner Signature
 Applicant Signature

Signature of Registered U.S. Patent Practitioner			
Signature	Andrew T. Pouzeshi/	Date (YYYY-MM-DD)	2016-08-31
Name	Andrew T. Pouzeshi	Registration Number	67672

This collection of information is required by 37 CFR 1.114. 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 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.

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

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether 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:	14270069			
Filing Date:	05-May-2014			
Title of Invention:	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS			
First Named Inventor/Applicant Name:	Joseph Jaroch			
Filer:	Andrew T. Pouzeshi/Jacquelyn Slate			
Attorney Docket Number:	04584.0021USU1			
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:				

IPR2023-00126

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
RCE- 1st Request	1801	1	1200	1200
Total in USD (\$)				1200

Electronic Acknowledgement Receipt

EFS ID:	26807224
Application Number:	14270069
International Application Number:	
Confirmation Number:	9580
Title of Invention:	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS
First Named Inventor/Applicant Name:	Joseph Jaroch
Customer Number:	23552
Filer:	Andrew T. Pouzeshi/Jacquelyn Slate
Filer Authorized By:	Andrew T. Pouzeshi
Attorney Docket Number:	04584.0021USU1
Receipt Date:	31-AUG-2016
Filing Date:	05-MAY-2014
Time Stamp:	20:23:46
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$ 1200
RAM confirmation Number	6337
Deposit Account	
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

IPR2023-00126

CrowdStrike EX1010 Page 39

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		2016-08-31-RespFOA-of-053116-04584-0021USU1.pdf	166215	yes	13
			4365b7e7c2ab428f8a3ae1909af87ef28be30dd8		
	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	13	
Warnings:					
Information:					
2	Request for Continued Examination (RCE)	2016-08-31-RCE-04584-0021USU1.pdf	697613	no	3
			55f12dcf4c7cb8415e0450539b6ef2b51b0fd536		
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30889	no	2
			d87d14b61028d76da4e6eeedd5976caa196e26c7		
Warnings:					
Information:					
Total Files Size (in bytes):			894717		

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Jaroach, et al.	Examiner:	Shehni, Ghazal B.
Serial No.:	14/270,069	Group Art Unit:	2436
Filed:	May 5, 2014	Docket No.:	04584.0021USU1
Title:	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS		

AMENDMENT & RESPONSE TO FINAL OFFICE ACTION

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

Dear Commissioner:

In response to the Final Office Action mailed May 31, 2016, 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 defining an action of a first object acting on a target;
generating a contextual state for at least one of the one or more events by correlating the at least one event to an originating object, the contextual state including an indication of the originating object of the first object and an indication of at least one of a device on which the first object is executed and a user associated with the first object;
obtaining a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object, the information including at least one of age, popularity, a determination as to whether the first object is malware, a determination as to whether the originating object is malware, Internet Protocol (IP) Address, and Uniform Resource Locator (URL) information, wherein the global perspective for one or more related events to the at least one event across a network;
assembling an event line including details associated with the at least one event, the details including information uniquely identifying the first object, the action of the first object, the target, and the originating object; and
transmitting the 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. (Original) The method of claim 1, further comprising:
obtaining an event priority based on one or more of the generated context and the global perspective for the at least one event, wherein the event line further includes the event priority for the at least one event.

4. (Original) 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. (Previously Presented) The method of claim 4, further comprising:
determining whether a global perspective for the at least one event has been cached;
when the global perspective for the at least one event has been cached, determining whether a time-to-live (TTL) value has been exceeded; and
when the global perspective for the at least one event has not been cached, obtaining a global perspective for the at least one event from a community database.
6. (Original) The method of claim 5, further comprising:
determining whether the cached global perspective for the at least one event has expired;
and
when the global perspective for the at least one event has expired, obtaining a global perspective for the at least one event from a community database.
7. (Original) The method of claim 4, further comprising:
heuristically displaying information identifying the first object performing the action, information identifying the action being performed, information identifying the target upon which the act is being performed, and the global perspective according to one or more of a location associated with the first object; at least one characteristic of an outbound connection associated with the first object; a dropped executable file; an age of the first object; and a number of concurrent connections associated with the first object.
8. (Canceled)
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 defining an action of a first object acting on a target;
generate a contextual state for at least one of the one or more events by
correlating the at least one event to an originating object, the contextual state including an indication of the originating object of the first object and an indication of at least one of a device on which the first object is executed and a user associated with the first object;

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

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

transmit the assembled event line utilizing the communication interface.

10. (Original) The system of claim 9, wherein the at least one of the one or more events 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. (Original) The system of claim 8, wherein the sensor agent is further operable to:
cache the one or more events; and
asynchronously consolidate and normalize the one or more events.
13. (Original) 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, determining whether a time-to-live (TTL) value has been exceeded; and
when the global perspective for the at least one event has not been cached, obtain a global perspective for the at least one event from a community database.
15. (Original) The system of claim 14, wherein the sensor agent is further operable to:
determine whether the cached global perspective for the at least one event has expired;
and
when the global perspective for the at least one event has expired, obtain a global perspective for the at least one event from a community database.
16. (Original) The system of claim 13, wherein the end recipient heuristically displays information identifying the first object performing the action, information identifying the action being performed, information identifying the target upon which the act is being performed, and

the global perspective according to one or more of a location associated with the first object; at least one characteristic of an outbound connection associated with the first object; a dropped executable file; an age of the first object; and a number of concurrent connections associated with the first object.

17. (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 defining an action of a first object acting on a target;

generate a contextual state for at least one of the one or more events by

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

assemble an event line including details associated with the at least one event, the details including information uniquely identifying each of the first object, the action of the first object, the target, [[and]] the originating object, and global perspective information comprising information about one or more related events to the one or more events across a network; and

transmit the assembled event line utilizing the communication interface.

18. (Previously Presented) 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, Internet Protocol (IP) Address, and Uniform Resource Locator (URL) information;

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

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

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

20. (Previously Presented) 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, Internet Protocol (IP) Address, and 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 final Office Action dated May 31, 2016, hereinafter “Office Action.” In that Office Action, claims 1-7 and 9-20 were examined and claims 1-7 and 9-19 were rejected. Specifically, claim 20 was objected to for various informalities. Claim 14 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. Claims 1-7 and 9-20 were rejected under 35 U.S.C. § 102(a)(2) as allegedly anticipated by Kumar et al. (U.S. Publ. No. 2013/0298244; hereinafter “Kumar”).

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, 9, 14, and 17 have been amended and no claims have been canceled or added. Therefore, claims 1-7 and 9-20 remain present for examination.

Allowable Subject Matter:

Claim 20 is indicated in the Office Action as allowable if rewritten in independent form. Applicants acknowledge with appreciation that the subject matter of claim 20 was found to be allowable. Applicants acknowledge the identification of allowable subject matter with appreciation.

Claim Rejections under 35 U.S.C. § 112:

Claim 14 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. Claim 14 has been amended to recite “the global perspective.” In light of this amendment, Applicants respectfully request that Examiner withdraw the rejection and allow claim 14.

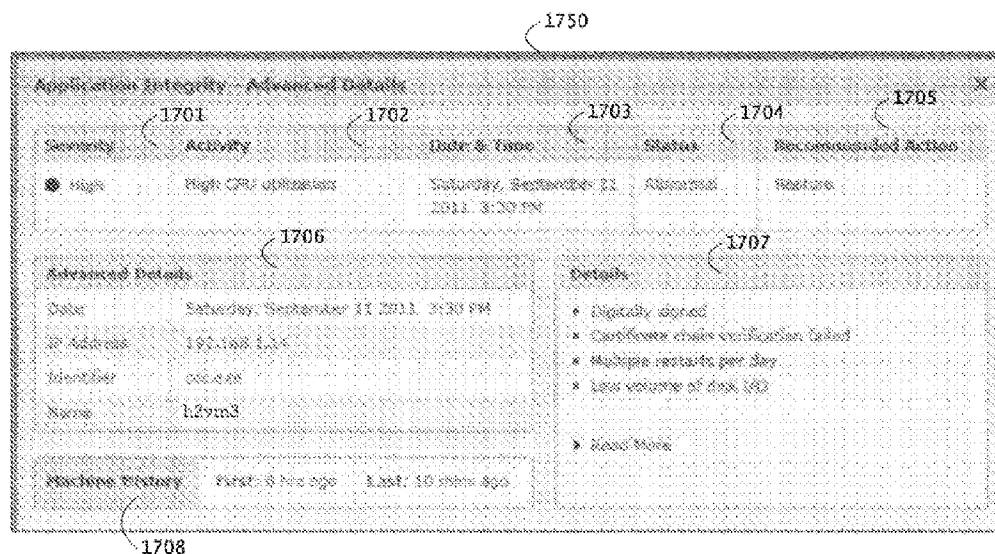
Claim Rejections under 35 U.S.C. § 102:

Claims 1-7 and 9-20 were rejected under 35 U.S.C. § 102(a)(2) as allegedly anticipated by Kumar. Applicants respectfully traverse this rejection because either the Examiner failed to state a *prima facie* case of anticipation or the current amendments to the claims now render the Examiner's arguments moot. "Anticipation requires the presence in a single prior art reference disclosure of each and every element of the claimed invention, arranged as in the claim."

Lindemann Mashinenfabrik GmbH v. Am. Hoist & Derrick Co., 730 F.2d 1452, 1458 (Fed. Cir. 1984); *see also*, MPEP § 2131. Applicants submit that the cited reference does not disclose all of the elements of the rejected claims.

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

Kumar relates to methods for threat identification and remediation. Kumar teaches a security orchestration service that generates runtime operational integrity profiles representing and identifying a level of threat or contextual trustworthiness of subjects and applications on the instrumented target platform. Kumar also teaches a method for threat identification and remediation for computing platforms based upon reconnaissance-based intelligence correlation and network/application monitoring are disclosed. The method comprises receiving: a dynamic context including endpoint events and network endpoint assessments; generating temporal events based on the network endpoint assessments; and correlating the endpoint events and temporal events before generating an integrity profile for the system. Kumar also discloses a GUI for tracking the application integrity, as reproduced below.



Turning now to the claims, Kumar fails to teach or suggest at least “obtaining a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object, the information including at least one of age, popularity, a determination as to whether the first object is malware, a determination as to whether the originating object is malware, Internet Protocol (IP) Address, and Uniform Resource Locator (URL) information, wherein the global perspective for one or more related events to the at least one event across a network,” as recited in independent claim 1. The Office Action argues that Kumar’s GUI, reproduced above, teaches this feature. Applicants respectfully disagree. Kumar’s GUI presents information related to the integrity of a single application running on a single device. There is no information displayed about events related to the application integrity across other devices on a network. Therefore, Kumar cannot possibly teach or suggest a “global perspective for one or more related events to the at least one event across a network,” as recited in independent claim 1. As such, Applicants respectfully request that the Examiner withdraw the § 102 rejection of claim 1.

The other independent claims recite similar limitations and are allowable over Kumar for at least the same or similar reasons. For example, claim 9 recites, *inter alia*:

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, Internet Protocol (IP) Address, and Uniform Resource Locator (URL) information, wherein the global perspective for one or more related events to the at least one event across a network...

Amended claim 17 recites, *inter alia*:

assemble an event line including details associated with the at least one event, the details including information uniquely identifying each of the first object, the action of the first object, the target, the originating object, and global perspective information comprising information about one or more related events to the one or more events across a network...

As such, claims 9 and 17 are not anticipated by Kumar.

The dependent claims, i.e. claims 2-8, 10-16 and 18-19, incorporate all of the limitations of the above independent claims, respectively, and are allowable over Kumar for at least the same reasons. As such, Applicants respectfully request that the Examiner withdraw the rejection and allow claims 1-7 and 9-20 at the Examiner's earliest convenience.

CONCLUSION

This Amendment fully responds to the Office Action mailed on May 31, 2016. 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.

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: August 31, 2016



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



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.
14/270,069	05/05/2014	Joseph Jaroch	04584.0021USU1	9580
23552	7590	05/31/2016	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
			05/31/2016	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. 14/270,069	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 03/16/2016.
☐ 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) 1-7 and 9-20 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) 1-7 and 9-19 is/are rejected.
- 8) ☒ Claim(s) 20 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 ____. | 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 03/16/2016. Claim 8 is canceled. Claims 1, 5, 9, 11, 14, 18, 20 have been amended. Therefore, claims 1-7, 9-20 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 (except claim 14), 35 USC 112, fourth paragraph rejections set forth in the previous office action.

Response to Arguments

Applicant's arguments filed 03/16/2016 have been fully considered but they are not persuasive. In the remark, Applicant argues that (1) Kumar fails to teach "...generating a contextual state for at least one of the one or more events", (2) Kumar fails to teach "...obtaining a global perspective for the at least one event".

In response to argument (1), Examiner respectfully disagrees. Kumar discloses the integrity processor can be configured to receive integrity events from runtime monitor that describes process, processor, system and binary analysis events...the rows in the event correlation matrix represent an application instance on the device...see Kumar, par. 135. Therefore Examiner maintains that Kumar does disclose this limitation.

Applicant's representative is invited to contact the Examiner with any questions.

In response to argument (2), Examiner respectfully disagrees. Kumar discloses runtime operational integrity monitoring console displays information including severity activity, an evaluation status, a timestamp corresponding to the displayed threat details pane, threat (or malware) identifier..., see Kumar par. 230-231. Therefore Examiner maintains that Kumar does disclose this limitation.

Allowable Subject Matter

2. Claim 20 is 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 § 112

3. The following is a quotation of 35 U.S.C. 112(b):
(b) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:
The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

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

5. Claim 14 recites "...determine whether **a global perspective** for the at least one even has been cached...". There is insufficient antecedent basis for these limitations. Appropriate correction is required.

6.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(a)(2) the claimed invention was described in a patent issued under section 151, or in an application for patent published or deemed published under section 122(b), in which the patent or application, as the case may be, names another inventor and was effectively filed before the effective filing date of the claimed invention.

Art Unit: 2436

8. Claims 1-7, 9-20 are rejected under 35 U.S.C. 102(a)(2) as being anticipated by Kumar et al (Pub. No. US 2013/0298244).

As per claim 1, Kumar discloses a method comprising:

gathering one or more events defining an action of a first object acting on a target (...receiving temporal events generated by the trust broker that measure the integrity of the system at last scan, and endpoint events from the endpoint trust agent...see par. 114);

generating a contextual state for at least one of the one or more events by correlating the at least one event to an originating object, the contextual state including an indication of the originating object of the first object and an indication of at least one of a device on which the first object is executed and a user associated with the first object (...the system event correlator can be configured to map the events to a cell in the risk correlation matrix grid....and to evaluate threats by category...see par. 114, 116, 135);

obtaining a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object, the information including at least one of age, popularity, a determination as to whether the first object is malware, a determination as to whether the originating object is malware, Internet Protocol (IP) Address, and Uniform Resource Locator (URL) information (...risk correlation matrix illustrates that for each device uniquely identified by a machine identifier (e.g. a virtual machine universally unique identifier, IP address...by mapping alerts to a behavior model threats may be classified...see par. 131, 230-231);

assembling an event line including details associated with the at least one event, the details including information uniquely identifying the first object, the action of the first object, the target, and the originating object; and transmitting the assembled event line (...generating a network security scan report, an endpoint collator to parse a plurality of received reports for categorization by package and component, an integrity processor...an endpoint trust agent, ...a threat classifier...the trust supervisor can be configured to receive infection profiles...see par. 169, 171).

As per claim 9, Kumar discloses system for providing forensic visibility into a system, comprising: a device including:

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

gather one or more events defining an action of a first object acting on a target (...receiving temporal events generated by the trust broker that measure the integrity of the system at last scan, and endpoint events from the endpoint trust agent...see par. 114);

generate a contextual state for at least one of the one or more events by correlating the at least one event to an originating object, the contextual state including an indication of the originating object of the first object and an indication of at least one of a device on which the first object is executed and a user associated with the first object (...the system event correlator can be configured to map the events to a cell in the risk correlation matrix grid....and to evaluate threats by category...see par. 114, 116, 135);

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, Internet Protocol (IP) Address, and Uniform Resource Locator (URL) information (...risk correlation matrix illustrates that for each device uniquely identified by a machine identifier (e.g. a virtual machine universally unique identifier, IP address...by mapping alerts to a behavior model threats may be classified...see par. 131, 230-231);

Art Unit: 2436

assemble an event line including details associated with the at least one event, the details including information uniquely identifying each of the first object, the action of the first object, the target, and the originating object; and transmit the assembled event line utilizing the communication interface (...generating a network security scan report, an endpoint collator to parse a plurality of received reports for categorization by package and component, an integrity processor...an endpoint trust agent, ...a threat classifier...the trust supervisor can be configured to receive infection profiles...see par. 169, 171).

As per claim 17, Kumar discloses system for providing forensic visibility into a system, comprising: a device including: a communication interface; a processor; data storage; and a sensor agent stored on the data storage that is executable by the processor, wherein the sensor agent is operable to: gather one or more events defining an action of a first object acting on a target (...receiving temporal events generated by the trust broker that measure the integrity of the system at last scan, and endpoint events from the endpoint trust agent...see par. 114); **generate a contextual state for at least one of the one or more events by correlating the at least one event to an originating object, the contextual state including an indication of the originating object of the first object and an indication of at least one of a device on which the first object is executed and a user associated with the first object** (...the system event correlator can be configured to map the events to a cell in the risk correlation matrix grid....and to evaluate threats by category...see par. 114, 116, 135); **assemble an event line including details associated with the at least one event, the details including information uniquely identifying each of the first object, the action of the first object, the target, and the originating object; and transmit the assembled event line utilizing the communication interface** (...generating a network security scan report, an endpoint collator to parse a plurality of received reports for categorization by package and component, an integrity processor...an endpoint trust agent, ...a threat classifier...the trust supervisor can be configured to receive infection profiles...see par. 169, 171).

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

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

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

As per claim 5, Kumar discloses determining whether a global perspective for the at least one event has been cached; when the global perspective for the at least one event has been cached, determining whether a time-to-live (TTL) value has been exceeded; and when the global perspective for the at least one event has not been cached, obtaining a global perspective for the at least one event from a community database (see par. 169, 174).

Art Unit: 2436

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

As per claim 7, Kumar discloses heuristically displaying information identifying the first object performing the action, information identifying the action being performed, information identifying the target upon which the act is being performed, and the global perspective according to one or more of a location associated with the first object; at least one characteristic of an outbound connection associated with the first object; a dropped executable file; an age of the first object; and a number of concurrent connections associated with the first object (see par. 131, 169, 171).

As per claim 10, Kumar discloses wherein the at least one of the one or more events is executed by the processor.

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

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

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

As per claim 14, Kumar discloses wherein the sensor agent is further operable to: determine whether a global perspective for the at least one event has been cached; when the global perspective for the at least one event has been cached, determining whether a time-to-live (TTL) value has been exceeded; and when the global perspective for the at least one event has not been cached, obtain a global perspective for the at least one event from a community database (see par. 169, 174).

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

Art Unit: 2436

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

As per claim 18, Kumar discloses a global perspective information server including: a processor; a communication interface; data storage; and a global perspective module, wherein the global perspective module is operable to: receive the event line from the device (...the system event correlator can be configured to map the events to a cell in the risk correlation matrix grid....and to evaluate threats by category...see par. 114, 116); obtain a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object, the information including at least one of age, popularity, a determination as to whether the first object is malware, a determination as to whether the originating object is malware, Internet Protocol (IP) Address, and Uniform Resource Locator (URL) information (...risk correlation matrix illustrates that for each device uniquely identified by a machine identifier (e.g. a virtual machine universally unique identifier, IP address...by mapping alerts to a behavior model threats may be classified...see par. 131); assemble a second event line including details associated with the at least one event, the details including information uniquely identifying each of the first object, the action of the first object, the target, and the originating object; and transmit the assembled second event line utilizing the communication interface to an end recipient (...generating a network security scan report, an endpoint collator to parse a plurality of received reports for categorization by package and component, an integrity processor...an endpoint trust agent, ...a threat classifier...the trust supervisor can be configured to receive infection profiles...see par. 169, 171).

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

9. **THIS ACTION IS MADE FINAL.** 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

Art Unit: 2436

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 mailing 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.

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.

Application/Control Number: 14/270,069
Art Unit: 2436

Page 10

/GHAZAL SHEHNI/
Primary Examiner, Art Unit 2436

Search Notes 	Application/Control No. 14270069	Applicant(s)/Patent Under Reexamination JAROCH ET AL.
	Examiner GHAZAL SHEHNI	Art Unit 2436

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
726	All	9/2/2015	GS

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor search (see search history printout)	9/2/2015	GS
East (see search history printout)	9/2/2015	GS
class 726 with text search	9/2/2015	GS
East (see search history printout)	5/24/2016	GS

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

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

EAST Search History

EAST Search History (Prior Art)

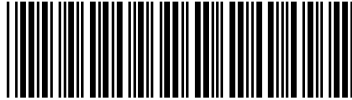
Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S20	111	(network with event) with sniffers	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2016/05/24 12:53
S21	1993	(analy\$4 or captur\$3 or record\$3) with (event with (network or traffic or web or packet or flow)) with security	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2016/05/24 13:45
S22	652	(analy\$4 or captur\$3 or record\$3) with (event with (network or traffic or web or packet or flow)) with security and "726".clas.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2016/05/24 13:45
S23	578	(analy\$4 or captur\$3 or record\$3) with (event with (network or packet or flow)) with security and "726".clas.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2016/05/24 13:46
S24	508	(analy\$4 or captur\$3 or record\$3) with (event with (network)) with security and "726".clas.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2016/05/24 13:46
S25	291	(analy\$4 or captur\$3 or record\$3) near7 (event with (network)) with security and "726".clas.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2016/05/24 13:46
S26	15	(analy\$4 or captur\$3 or record\$3) near7 (event with (network)) with security with (sniffer or malicious or virus or trojan or spy\$ware)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2016/05/24 13:47

EAST Search History (Interference)

<This search history is empty>

5/ 24/ 2016 9:03:27 PM

C:\ Users\ gshehni\ Documents\ EAST\ Workspaces\ 14270069.wsp

<i>Index of Claims</i> 	Application/Control No. 14270069	Applicant(s)/Patent Under Reexamination JAROCK 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	09/02/2015	05/24/2016						
	1	✓	✓						
	2	✓	✓						
	3	✓	✓						
	4	✓	✓						
	5	✓	✓						
	6	✓	✓						
	7	✓	✓						
	8	✓	-						
	9	✓	✓						
	10	✓	✓						
	11	✓	✓						
	12	✓	✓						
	13	✓	✓						
	14	✓	✓						
	15	✓	✓						
	16	✓	✓						
	17	✓	✓						
	18	✓	✓						
	19	✓	✓						
	20	O	O						



UNITED STATES PATENT AND TRADEMARK OFFICE

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

BIB DATA SHEET

CONFIRMATION NO. 9580

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.		
14/270,069	05/05/2014	726	2436	04584.0021USU1		
APPLICANTS Webroot Inc., Broomfield, CO;						
INVENTORS Joseph Jaroch, Deer Park, IL; Jacques Etienne Erasmus, Belper, UNITED KINGDOM; Paul Barnes, Derby, UNITED KINGDOM; Johannes Mayr, Linz, AUSTRIA; Michael Leidesdorff, Niwot, CO; Marco Giuliani, Bastia Umbra (PG), ITALY; Christopher Jon Williams, Derbyshire, UNITED KINGDOM; Chad Edward Bacher, Arvada, CO;						
** CONTINUING DATA ***** This appln claims benefit of 61/819,470 05/03/2013						
** FOREIGN APPLICATIONS *****						
** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ** 05/13/2014						
Foreign Priority claimed ☐ Yes ☒ No 35 USC 119(a-d) conditions met ☐ Yes ☒ No Verified and /GHAZAL B SHEHNI/ Acknowledged Examiner's Signature		☐ Met after Allowance Initials	STATE OR COUNTRY IL	SHEETS DRAWINGS 15	TOTAL CLAIMS 20	INDEPENDENT CLAIMS 3
ADDRESS MERCHANT & GOULD P.C. P.O. BOX 2903 MINNEAPOLIS, MN 55402-0903 UNITED STATES						
TITLE METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS						
FILING FEE RECEIVED 800	FEES: Authority has been given in Paper No. _____ to charge/credit DEPOSIT ACCOUNT No. _____ for following:			☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit		



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	REQUEST ID
14/270,069	05/05/2014	Webroot Inc.	04584.0021USU1	18075

Acknowledgement of Loss of Entitlement to Entity Status Discount

The entity status change request below filed through Private PAIR on 05/17/2016 has been accepted.

CERTIFICATIONS:

Change of Entity Status:

× Applicant changing to regular undiscounted fee status.

NOTE: Checking this box will be taken to be notification of loss of entitlement to small or micro entity status, as applicable.

This portion must be completed by the signatory or signatories making the entity status change in accordance with 37 CFR 1.4(d)(4).

Signature:	/Andrew T. Pouzeshi/
Name:	Andrew T. Pouzeshi
Registration Number:	67672

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Jaroach, et al.	Examiner:	Shehni, Ghazal B.
Serial No.:	14/270,069	Group Art Unit:	2436
Filed:	May 5, 2014	Docket No.:	04584.0021USU1
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 September 16, 2015, 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 defining an action of a first object acting on a target;
generating a contextual state for at least one of the one or more events by correlating the at least one event to an originating object, the contextual state including an indication of the originating object of the first object and an indication of at least one of a device on which the first object is executed and a user associated with the first object;
obtaining a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object, the information including at least one of age, popularity, a determination as to whether the first object is malware, a determination as to whether the originating object is malware[[: and]], Internet Protocol (IP) Address, and [[or]] Uniform Resource Locator (URL) information;
assembling an event line including details associated with the at least one event, the details including information uniquely identifying ~~each of~~ the first object, the action of the first object, the target, and the originating object; and
transmitting the assembled event line.
2. (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. (Original) The method of claim 1, further comprising:
obtaining an event priority based on one or more of the generated context and the global perspective for the at least one event, wherein the event line further includes the event priority for the at least one event.

4. (Original) 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 global perspective for the at least one event has been cached;
when the global perspective for the at least one event has been cached, ~~obtaining a global perspective for the at least one event based on the cached global perspective~~ determining whether a time-to-live (TTL) value has been exceeded; and
when the global perspective for the at least one event has not been cached, obtaining a global perspective for the at least one event from a community database.
6. (Original) The method of claim 5, further comprising:
determining whether the cached global perspective for the at least one event has expired;
and
when the global perspective for the at least one event has expired, obtaining a global perspective for the at least one event from a community database.
7. (Original) The method of claim 4, further comprising:
heuristically displaying information identifying the first object performing the action, information identifying the action being performed, information identifying the target upon which the act is being performed, and the global perspective according to one or more of a location associated with the first object; at least one characteristic of an outbound connection associated with the first object; a dropped executable file; an age of the first object; and a number of concurrent connections associated with the first object.
8. (Canceled)

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 defining an action of a first object acting on a target;

generate a contextual state for at least one of the one or more events by

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

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

Internet Protocol (IP) Address, and [[or]] Uniform Resource Locator (URL) information;

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

transmit the assembled event line utilizing the communication interface.

10. (Original) The system of claim 9, wherein the 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. (Original) The system of claim 8, wherein the sensor agent is further operable to:
cache the one or more events; and
asynchronously consolidate and normalize the one or more events.
13. (Original) 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 global perspective for the at least one event has been cached;
when the global perspective for the at least one event has been cached, ~~obtaining a global perspective for the at least one event based on the cached global perspective~~ determining whether a time-to-live (TTL) value has been exceeded; and
when the global perspective for the at least one event has not been cached, obtain a global perspective for the at least one event from a community database.
15. (Original) The system of claim 14, wherein the sensor agent is further operable to:
determine whether the cached global perspective for the at least one event has expired;
and
when the global perspective for the at least one event has expired, obtain a global perspective for the at least one event from a community database.
16. (Original) The system of claim 13, wherein the end recipient heuristically displays information identifying the first object performing the action, information identifying the action

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

17. (Original) A system for providing forensic visibility into a system, comprising:
 - a device including:
 - a communication interface;
 - a processor;
 - data storage; and
 - a sensor agent stored on the data storage that is executable by the processor, wherein the sensor agent is operable to:
 - gather one or more events defining an action of a first object acting on a target;
 - generate a contextual state for at least one of the one or more events by correlating the at least one event to an originating object, the contextual state including an indication of the originating object of the first object and an indication of at least one of a device on which the first object is executed and a user associated with the first object;
 - assemble an event line including details associated with the at least one event, the details including information uniquely identifying each of the first object, the action of the first object, the target, and the originating object; and
 - transmit the assembled event line utilizing the communication interface.
18. (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, and [[or]] Uniform Resource Locator (URL) information;
assemble a second event line including details associated with the at least one event, the details including information uniquely identifying each of the first object, the action of the first object, the target, and the originating object; and
transmit the assembled second event line utilizing the communication interface to an end recipient.

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

20. (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, and [[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 September 16, 2015, hereinafter “Office Action.” In that Office Action, claims 1-20 were examined and claims 1-19 were rejected. Claim 20 was objected to. Claims 1, 3, 4, 7-10, 12, 13, 16 and 17-19 were 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 1-19 were rejected under 35 U.S.C. § 102(a)(2) as allegedly anticipated by Kumar et al. (U.S. Publ. No. 2013/0298244; hereinafter “Kumar”).

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, 5, 9, 11, 14, 18 and 20 have been amended, claim 8 has been canceled, and no claims have been added. Therefore, claims 1-7 and 9-20 remain present for examination.

Allowable Subject Matter

Claim 20 is indicated in the Office Action as allowable if rewritten in independent form. Applicants acknowledge with appreciation that the subject matter of claim 20 was found to be allowable.

Claim Rejections under 35 U.S.C. § 101:

Claims 1, 3, 4, 7-10, 12, 13, 16, and 17-19 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 are directed to the abstract idea of generating a contextual state for one or more events. The claims presented herein, however, do not merely recite an abstract idea, and under the recently-issued Interim Guidance and the *Alice* decision, Applicants respectfully traverse the rejection.

The current claims do not recite an abstract idea. Rather, the claims are directed to solving a technical problem. Typically, network forensic systems use network forensic tools (e.g., network sniffers and packet capture tools) to detect and capture information associated with communication sessions. Although such network forensic tools are operable to passively collect network traffic, the tools reside at a network edge (e.g., outside of a system or hosts). As a result, the network forensic tools have no ability to obtain useful information within a host or to establish any sort of context from within a host that is generating and/or receiving network events. To address this, aspects of the present disclosure enable methods for providing forensic visibility into systems and networks. For example, a local aggregator/interpreter, context analyzer and sensor agent may provide visibility into occurrences across an environment to ensure that a user (e.g., an administrator) is aware of any system change and data communications in and out of the computing devices residing on the network. During this process, identified events may be correlated to objects, thus creating an audit trail for each individual event. A global perspective for identified events may then be generated using the event and object data. Such a solution is not an abstract idea and is drastically different from the broad and unrestricted abstract ideas of “the fundamental economic practice” of hedging in *Bilski*, the concept of intermediated settlement in *Alice*, and the mathematical formulas of *Benson* and *Flook*.

To the extent there is any abstract idea involved in the claimed invention, the Supreme Court explicitly stated that such involvement does not prevent the claims from being patent eligible. The Supreme Court warned that the exclusionary principle must be construed narrowly “lest it swallow all of patent law,” explaining:

At some level, “all inventions . . . embody, use, reflect, rest upon, or apply laws of nature, natural phenomena, or abstract ideas.” *Id.*, at ___, 132 S. Ct. 1289, 182 L. Ed. 2d 321, 327). Thus, an invention is not rendered ineligible for patent simply because it involves an abstract concept. *See Diamond v. Diehr*, 450 U.S. 175, 187, 101 S. Ct. 1048, 67 L. Ed. 2d 155 (1981). “[A]pplication[s]” of such concepts “‘to a new and useful end,’” we have said, remain eligible for patent protection. *Gottschalk v. Benson*, 409 U.S. 63, 67, 93 S. Ct. 253, 34 L. Ed. 2d 273 (1972).

Alice, 134 S. Ct. at 2354. The MPEP itself reiterates that same narrow treatment of the abstract idea exclusions: “If the record as a whole suggests that it is more likely than not that the claimed

invention would be considered a practical application of an abstract idea, physical phenomenon, or law of nature, then USPTO personnel should not reject the claim.” MPEP §2106.

Furthermore, even assuming, *arguendo*, that the claimed invention is found to be directed to an abstract idea, the Applicants respectfully submit that the pending claims include claim features that provide features that amount to significantly more than a judicial exception. Pages 20-22 of the USPTO guidelines on Patent Subject Matter issued on December 16, 2014 (further updated in July 2015) provide guidance on what amounts to significantly more than a judicial exception and thus applies the invention in a meaningful way:

... The Supreme Court has identified a number of considerations for determining whether a claim with additional elements amounts to significantly more than the judicial exception itself. The following are examples of these considerations, which are not intended to be exclusive or limiting. Limitations that may be enough to qualify as “significantly more” when recited in a claim with a judicial exception include:

- Improvements to another technology or technical field
- Improvements to the functioning of the computer itself;
- Applying the judicial exception with, or by use of, a particular machine
- Effecting a transformation or reduction of a particular article to a different state or thing;
- Adding a specific limitation other than what is well-understood, routine and conventional in the field, or adding unconventional steps that confine the claim to a particular useful application; or
- Other meaningful limitations beyond generally linking the use of the judicial exception to a particular technological environment.

As is clear from the language above, the USPTO guidelines recognize that claimed inventions recite “significantly more” when describing transformation or reduction of a particular article to a different state or thing. In this case, the claimed invention provides for determining correlations between events and objects, and creating an audit trail for each individual event. For example, a context analyzer may correlate an actor, victim, and/or event type to one or more originating processes, devices, and users. After the analysis is complete, a sensor agent may use the correlated data to generate a global perspective for each event such that an administrator is able to forensically track back any event which occurs to what triggered it.

Thus, the global perspective represents a drastic transformation of raw event data into a comprehensive, system-wide forensic audit trail.

Furthermore, the USPTO guidelines recognize that claimed inventions recite “significantly more” when describing improvements to the functioning of the computer itself. In this case, examples of the claimed systems and methods provide low level system filters which intercept system events “in a manner such that the operation of the system filter does not impact system performance.” *Specification*, para. [0008]. For example, on an average system, because tens of millions of events take place every minute, the noise ratio can prevent forensic solutions from being able to provide sufficient value to the end consumer of their data due to the inability to quickly find important events. A product which impacts system performance will have considerably diminished value to an administrator and can negatively affect the results of an analysis undertaken. Examples of the present systems and methods address this shortcoming by providing a system filter that substantially improves the system performance of the computing devices in the system.

As such, Applicants respectfully submit that claims 1, 3, 4, 7-10, 12, 13, 16 and 17-19 recite statutory subject matter and request that the Examiner withdraw the rejection and allow claims 1, 3, 4, 7-10, 12, 13, 16 and 17-19 at the Examiner’s earliest convenience.

Claim Rejections under 35 U.S.C. § 112:

Claims 5, 11 and 14

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. Claims 5 and 14 have been amended to recite “when the global perspective for the at least one event has been cached, *determining whether a time-to-live (TTL) value has been exceeded.*” Claim 11 has been amended to recite “and the sensor agent transmits the event line to the end recipient *device.*” In light of these amendments, Applicants respectfully request that Examiner withdraw the rejection and allow claims 5, 11 and 14.

Claim 8

Claim 8 was rejected under 35 U.S.C. § 112, fourth paragraph, for allegedly failing to particularly point out and distinctly claim the subject matter that Applicants regard as their invention. Claim 8 has been canceled without prejudice. As such, the rejection is moot.

Claim Rejections under 35 U.S.C. § 102:

Claims 1-19 were rejected under 35 U.S.C. § 102(a)(2) as allegedly anticipated by Kumar. Applicants respectfully traverse this rejection because either the Examiner failed to state a *prima facie* case of anticipation or the current amendments to the claims now render the Examiner's arguments moot. "Anticipation requires the presence in a single prior art reference disclosure of each and every element of the claimed invention, arranged as in the claim." *Lindemann Maschinenfabrik GmbH v. Am. Hoist & Derrick Co.*, 730 F.2d 1452, 1458 (Fed. Cir. 1984); *see also*, MPEP § 2131. Applicants submit that the cited reference does not disclose all of the elements of the rejected claims.

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

Kumar relates to methods for threat identification and remediation. Kumar teaches a security orchestration service that generates runtime operational integrity profiles representing and identifying a level of threat or contextual trustworthiness of subjects and applications on the instrumented target platform. Kumar also teaches a method for threat identification and remediation for computing platforms based upon reconnaissance-based intelligence correlation and network/application monitoring are disclosed. The method comprises receiving: a dynamic

context including endpoint events and network endpoint assessments; generating temporal events based on the network endpoint assessments; and correlating the endpoint events and temporal events before generating an integrity profile for the system.

Turning specifically to the claims, Kumar fails to teach at least “generating a contextual state for at least one of the one or more events,” as recited in claim 1. The Office Action refers to Kumar as disclosing mapping events to risk matrix correlation grid, and equates such disclosure to generating a contextual state for an event. *Office Action*, pg. 5. Applicants respectfully disagree with this interpretation of Kumar and the conclusions drawn therefrom. Instead, Applicants submit that the risk matrix correlation grid is used to correlate endpoint events to endpoint alerts:

The risk correlation matrix **721** can comprise a universally unique identifier (UUID) for the system, system warnings **723** mapped to at least one system warning class **722**, and at least a system warning class **722** to diagnose system deviations (i.e., system deviated integrity warnings **724**), system duress, system vulnerable and system infections (i.e., system infected integrity warnings **724**). *Kumar*, para. [0130].

As explained by Kumar, each event may produce one or more alerts. When an alert is produced, the risk matrix correlation grid is evaluated to determine a corresponding warning to trigger. However, Kumar does not teach or suggest that the risk matrix correlation grid comprises context state information for the event, as recited in the claims. That is, the risk matrix correlation grid does not comprise or otherwise relate to “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.” As such, Kumar fails to teach generating a contextual state for an event.

Furthermore, Kumar also fails to teach “obtaining a global perspective for the at least one event,” as recited in claim 1. The Office Action refers to Kumar as disclosing mapping events to a behavior model, and equates such disclosure to obtaining a global perspective for an event. *Office Action*, pg. 5. Applicants respectfully disagree with this interpretation of Kumar and the conclusions drawn therefrom. Instead, Applicants submit that the Kumar teaches grouping alerts into categories (e.g., platform, application, etc.) that are weighted by threat level. The alerts and

alert categories are then mapped to a behavior model to classify unknown threats without requiring image or wire level signatures. *Kumar*, para. [0131]. The behavior model may then use incoming alerts to identify potential threats. However, *Kumar* does not teach that the behavior model analyzes or produces information regarding an age of an object, a popularity of an object, a determination as to whether the object is malware, a determination as to whether the originating object is malware, Internet Protocol (IP) Address, or Uniform Resource Locator (URL) information. Accordingly, *Kumar* fails to teach the global perspective recited in the claims and claim 1 is not anticipated by *Kumar*.

The other independent claims recite similar limitations and are allowable over *Kumar* for at least the same or similar reasons. For example, claim 9 recites, *inter alia*:

generate a contextual state for at least one of the one or more events by correlating the at least one event to an originating object ...

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 ...

Amended claim 17 recites, *inter alia*:

generate a contextual state for at least one of the one or more events by correlating the at least one event to an originating object ...

As such, claims 9 and 17 are not anticipated by *Kumar*.

The dependent claims, i.e. claims 2-8, 10-16 and 18-19, incorporate all of the limitations of the above independent claims, respectively, and are allowable over *Kumar* for at least the same reasons. As such, Applicants respectfully request that the Examiner withdraw the rejection and allow claims 1-19 at the Examiner's earliest convenience.

CONCLUSION

This Amendment fully responds to the Office Action mailed on September 16, 2015. 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 Amendment. 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: March 16, 2016



/David D. Harrell/
David D. Harrell, Reg. No. 71,855
Merchant & Gould P.C.
P.O. Box 2903
Minneapolis, MN 55402-0903
(303) 357-1242

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)		Docket Number (Optional) 04584.0021USU1
Application Number 14/270069	Filed 05-05-2014	
For METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS		
Art Unit 2436	Examiner SHEHNI, GHAZAL B	

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above-identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

	Fee	Small Entity Fee	Micro Entity Fee	
☐ One month (37 CFR 1.17(a)(1))	\$200	\$100	\$50	\$ _____
☐ Two months (37 CFR 1.17(a)(2))	\$600	\$300	\$150	\$ _____
☒ Three months (37 CFR 1.17(a)(3))	\$1,400	\$700	\$350	\$ <u>1400</u>
☐ 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 71855.

☐ attorney or agent acting under 37 CFR 1.34. Registration number _____.

/David D. Harrell/ 2016-03-16
Signature Date

David D. Harrell 303-357-1242
Typed or printed name Telephone Number

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☒ * Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.136(a). The information is required to obtain or retain a benefit by the public, which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 6 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop PCT, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Electronic Patent Application Fee Transmittal

Application Number:	14270069			
Filing Date:	05-May-2014			
Title of Invention:	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS			
First Named Inventor/Applicant Name:	Joseph Jaroch			
Filer:	Andrew T. Pouzeschi/Elizabeth Pallardy			
Attorney Docket Number:	04584.0021USU1			
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:				

IPR2023-00126

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Extension - 3 months with \$0 paid	1253	1	1400	1400
Miscellaneous:				
Total in USD (\$)				1400

Electronic Acknowledgement Receipt

EFS ID:	25219204
Application Number:	14270069
International Application Number:	
Confirmation Number:	9580
Title of Invention:	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS
First Named Inventor/Applicant Name:	Joseph Jaroch
Customer Number:	23552
Filer:	Andrew T. Pouzeshi/Elizabeth Pallardy
Filer Authorized By:	Andrew T. Pouzeshi
Attorney Docket Number:	04584.0021USU1
Receipt Date:	16-MAR-2016
Filing Date:	05-MAY-2014
Time Stamp:	18:53:06
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$ 1400
RAM confirmation Number	5663
Deposit Account	132725
Authorized User	HARRELL, DAVID

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 CFR 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 CFR 1.17 (Patent application and reexamination processing fees)

IPR2023-00126

Charge any Additional Fees required under 37 CFR 1.19 (Document supply fees)

Charge any Additional Fees required under 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		04584_0021USU1_RespNFOA_of09-16-15.PDF	141188 24a4cfe479bf4337efb85c86324ee65add689b32	yes	16
	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	16	
Warnings:					
Information:					
2	Extension of Time	04584_0021USU1_EOT.PDF	102538 c822ab52eef73a03f2c676cd08ef3dc753cc6413	no	1
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	31414 a983ef4ac27109defb7a12895cf29a701619bbb0	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			275140		

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.
14/270,069	05/05/2014	Joseph Jaroch	04584.0021USU1	9580
23552	7590	09/16/2015	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
			09/16/2015	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. 14/270,069	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 05/05/2014.
☐ 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) 1-19 is/are rejected.
- 8) ☒ Claim(s) 20 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 05/05/2014 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

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

Certified copies:

- a) ☐ All b) ☐ Some** c) ☐ None of the:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

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

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b)
Paper No(s)/Mail Date _____
- 3) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 4) ☐ Other: _____

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

DETAILED ACTION

Claim Rejections - 35 USC § 112

2. The following is a quotation of 35 U.S.C. 112(b):
(b) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:
The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 5, 11 and 14 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.
4. Claims 5 and 14 recite "...when the global perspective for the at least one event has been cached, obtaining a global perspective for the at least one event...". There is insufficient antecedent basis for these limitations. Appropriate correction is required.

Art Unit: 2436

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

Claim Rejections - 35 USC § 101

6. Claims 1, 3, 4, 7, 8, 9, 10, 12, 13, 16, 17-19 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter because the claim(s) as a whole, considering all claim elements both individually and in combination, do not amount to significantly more than an abstract idea. The claim(s) is/are directed to the abstract idea of **generating a contextual state for at least one of the one or more events by correlating the at least one event...** The additional element(s) or combination of elements in the claim(s) other than the abstract idea per se amount(s) to no more than: **obtaining information associated with one or more of the first object and the originating object**. Viewed as a whole, these additional claim element(s) do not provide meaningful limitation(s) to transform the abstract idea into a patent eligible application of the abstract idea such that the claim(s) amounts to significantly more than the abstract idea itself. Also claim 8 recites "...a computer readable storage medium...". It appears that the medium recited in the claim 17 is not described in the specification as including a tangible medium in a manner which enables it to act as a computer component to realize the computer program's functionality. Therefore, when the claim is interpreted broadly as transmission medium or signal, the claim appear to be non-statutory because it is not tangibly embodied in a manner so as to be. Examiner suggests to Applicant to amend the claim to include "...at least one non transitory storage medium..." in the claim language. Therefore, the claims 1, 3, 4, 7, 8, 9, 10, 12, 13, 16, 17-19 are rejected under 35 U.S.C. 101 as being directed to non-statutory subject matter.

Claim Rejections - 35 USC § 112

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

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

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

Art Unit: 2436

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

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

Allowable Subject Matter

9. Claim 20 is 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 § 102

(a)(2) the claimed invention was described in a patent issued under section 151, or in an application for patent published or deemed published under section 122(b), in

Art Unit: 2436

which the patent or application, as the case may be, names another inventor and was effectively filed before the effective filing date of the claimed invention.

10. Claims 1-19 are rejected under 35 U.S.C. 102(a)(2) as being anticipated by Kumar et al (Pub. No. US 2013/0298244).

As per claim 1, Kumar discloses a method comprising:

gathering one or more events defining an action of a first object acting on a target (...receiving temporal events generated by the trust broker that measure the integrity of the system at last scan, and endpoint events from the endpoint trust agent...see par. 114);

generating a contextual state for at least one of the one or more events by correlating the at least one event to an originating object, the contextual state including an indication of the originating object of the first object and an indication of at least one of a device on which the first object is executed and a user associated with the first object (...the system event correlator can be configured to map the events to a cell in the risk correlation matrix grid....and to evaluate threats by category...see par. 114, 116);

obtaining a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object, the information including at least one of age, popularity, a determination as to whether the first object is malware, a determination as to whether the originating object is malware; and Internet Protocol (IP) Address or Uniform Resource Locator (URL) information (...risk correlation matrix illustrates that for each device uniquely identified by a machine identifier (e.g. a virtual machine universally unique identifier, IP address...by mapping alerts to a behavior model threats may be classified...see par. 131);

assembling an event line including details associated with the at least one event, the details including information uniquely identifying each of the first object, the action of the first object, the target, and the originating object; and transmitting the assembled event line (...generating a network security scan report, an endpoint collator to parse a plurality of received reports for categorization by package and component, an integrity processor...an endpoint trust agent, ...a threat classifier...the trust supervisor can be configured to receive infection profiles...see par. 169, 171).

As per claim 9, Kumar discloses system for providing forensic visibility into a system, comprising: a device including:

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

gather one or more events defining an action of a first object acting on a target (...receiving temporal events generated by the trust broker that measure the integrity of the system at last scan, and endpoint events from the endpoint trust agent...see par. 114);

generate a contextual state for at least one of the one or more events by correlating the at least one event to an originating object, the contextual state including an indication of the originating object of the first object and an indication of at least one of a device on which the first object is executed and a user associated with the first object (...the system event correlator can be configured to map the events to a cell in the risk correlation matrix grid....and to evaluate threats by category...see par. 114, 116);

Art Unit: 2436

obtain a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object, the information including at least one of age, popularity, a determination as to whether the first object is malware, a determination as to whether the originating object is malware; and Internet Protocol (IP) Address or Uniform Resource Locator (URL) information (...risk correlation matrix illustrates that for each device uniquely identified by a machine identifier (e.g. a virtual machine universally unique identifier, IP address...by mapping alerts to a behavior model threats may be classified...see par. 131);
assemble an event line including details associated with the at least one event, the details including information uniquely identifying each of the first object, the action of the first object, the target, and the originating object; and transmit the assembled event line utilizing the communication interface (...generating a network security scan report, an endpoint collator to parse a plurality of received reports for categorization by package and component, an integrity processor...an endpoint trust agent, ...a threat classifier...the trust supervisor can be configured to receive infection profiles...see par. 169, 171).

As per claim 17, Kumar discloses system for providing forensic visibility into a system, comprising: a device including: a communication interface; a processor; data storage; and a sensor agent stored on the data storage that is executable by the processor, wherein the sensor agent is operable to: gather one or more events defining an action of a first object acting on a target (...receiving temporal events generated by the trust broker that measure the integrity of the system at last scan, and endpoint events from the endpoint trust agent...see par. 114);
generate a contextual state for at least one of the one or more events by correlating the at least one event to an originating object, the contextual state including an indication of the originating object of the first object and an indication of at least one of a device on which the first object is executed and a user associated with the first object (...the system event correlator can be configured to map the events to a cell in the risk correlation matrix grid....and to evaluate threats by category...see par. 114, 116);
assemble an event line including details associated with the at least one event, the details including information uniquely identifying each of the first object, the action of the first object, the target, and the originating object; and transmit the assembled event line utilizing the communication interface (...generating a network security scan report, an endpoint collator to parse a plurality of received reports for categorization by package and component, an integrity processor...an endpoint trust agent, ...a threat classifier...the trust supervisor can be configured to receive infection profiles...see par. 169, 171).

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

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

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

Art Unit: 2436

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

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

As per claim 7, Kumar discloses heuristically displaying information identifying the first object performing the action, information identifying the action being performed, information identifying the target upon which the act is being performed, and the global perspective according to one or more of a location associated with the first object; at least one characteristic of an outbound connection associated with the first object; a dropped executable file; an age of the first object; and a number of concurrent connections associated with the first object (see par. 131, 169, 171).

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

As per claim 10, Kumar discloses wherein the at least one of the one or more events is executed by the processor.

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

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

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

As per claim 14, Kumar discloses wherein the sensor agent is further operable to: determine whether a global perspective for the at least one event has been cached; when the global perspective for the at least one event has been cached, obtain a global perspective for the at least one event based on the cached global perspective; and when the global perspective for the at least one event has not been cached, obtain a global perspective for the at least one event from a

Art Unit: 2436

community database (see par. 169, 174).

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

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

As per claim 18, Kumar discloses a global perspective information server including: a processor; a communication interface; data storage; and a global perspective module, wherein the global perspective module is operable to: receive the event line from the device (...the system event correlator can be configured to map the events to a cell in the risk correlation matrix grid....and to evaluate threats by category...see par. 114, 116); obtain a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object, the information including at least one of age, popularity, a determination as to whether the first object is malware, a determination as to whether the originating object is malware; and Internet Protocol (IP) Address or Uniform Resource Locator (URL) information (...risk correlation matrix illustrates that for each device uniquely identified by a machine identifier (e.g. a virtual machine universally unique identifier, IP address...by mapping alerts to a behavior model threats may be classified...see par. 131); assemble a second event line including details associated with the at least one event, the details including information uniquely identifying each of the first object, the action of the first object, the target, and the originating object; and transmit the assembled second event line utilizing the communication interface to an end recipient (...generating a network security scan report, an endpoint collator to parse a plurality of received reports for categorization by package and component, an integrity processor...an endpoint trust agent, ...a threat classifier...the trust supervisor can be configured to receive infection profiles...see par. 169, 171).

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

Conclusion

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

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

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

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

/GHAZAL SHEHNI/
Primary Examiner, Art Unit 2436

Notice of References Cited	Application/Control No. 14/270,069		Applicant(s)/Patent Under Reexamination JAROCH ET AL.	
	Examiner GHAZAL SHEHNI		Art Unit 2436	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-2013/0298244 A1	11-2013	KUMAR; Srinivas	G06F21/52	726/25
	B	US-				
	C	US-				
	D	US-				
	E	US-				
	F	US-				
	G	US-				
	H	US-				
	I	US-				
	J	US-				
	K	US-				
	L	US-				
	M	US-				

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

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

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



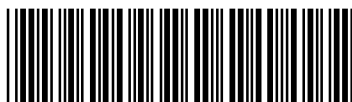
UNITED STATES PATENT AND TRADEMARK OFFICE

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

BIB DATA SHEET

CONFIRMATION NO. 9580

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.		
14/270,069	05/05/2014	726	2436	04584.0021USU1		
APPLICANTS Webroot Inc., Broomfield, CO;						
INVENTORS Joseph Jaroch, Deer Park, IL; Jacques Etienne Erasmus, Belper, UNITED KINGDOM; Paul Barnes, Derby, UNITED KINGDOM; Johannes Mayr, Linz, AUSTRIA; Michael Leidesdorff, Niwot, CO; Marco Giuliani, Bastia Umbra (PG), ITALY; Christopher Jon Williams, Derbyshire, UNITED KINGDOM; Chad Edward Bacher, Arvada, CO;						
** CONTINUING DATA ***** This appln claims benefit of 61/819,470 05/03/2013						
** FOREIGN APPLICATIONS *****						
** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ** ** SMALL ENTITY ** 05/13/2014						
Foreign Priority claimed ☐ Yes ☒ No 35 USC 119(a-d) conditions met ☐ Yes ☒ No Verified and Acknowledged <u>//</u> Examiner's Signature		☐ Met after Allowance Initials	STATE OR COUNTRY IL	SHEETS DRAWINGS 15	TOTAL CLAIMS 20	INDEPENDENT CLAIMS 3
ADDRESS MERCHANT & GOULD P.C. P.O. BOX 2903 MINNEAPOLIS, MN 55402-0903 UNITED STATES						
TITLE METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS						
FILING FEE RECEIVED 800	FEES: Authority has been given in Paper No. _____ to charge/credit DEPOSIT ACCOUNT No. _____ for following:			☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit		

<i>Index of Claims</i> 	Application/Control No. 14270069	Applicant(s)/Patent Under Reexamination JAROCK 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	09/02/2015							
	1	✓							
	2	✓							
	3	✓							
	4	✓							
	5	✓							
	6	✓							
	7	✓							
	8	✓							
	9	✓							
	10	✓							
	11	✓							
	12	✓							
	13	✓							
	14	✓							
	15	✓							
	16	✓							
	17	✓							
	18	✓							
	19	✓							
	20	O							

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	101	(network with event) with sniffers	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/09/02 15:57
L3	94	(network with event) with (analysis with forensic)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/09/02 15:58
L4	9	((network with event) with sniffers) with request	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/09/02 15:59
S1	6	((Joseph) near2 (Jaroch)).INV.	US-PGPUB; USPAT	ADJ	ON	2015/08/24 21:19
S2	2	((Jacques) near2 (Erasmus)).INV.	US-PGPUB; USPAT	ADJ	ON	2015/08/24 21:19
S3	52	((Paul) near2 (Barnes)).INV.	US-PGPUB; USPAT	ADJ	ON	2015/08/24 21:19
S4	7	((Johannes) near2 (Mayr)).INV.	US-PGPUB; USPAT	ADJ	ON	2015/08/24 21:19
S5	1	((Michael) near2 (Leidesdorff)).INV.	US-PGPUB; USPAT	ADJ	ON	2015/08/24 21:20
S6	13	((Marco) near2 (Giuliani)).INV.	US-PGPUB; USPAT	ADJ	ON	2015/08/24 21:20
S7	1291	((Christopher) near2 (Williams)).INV.	US-PGPUB; USPAT	ADJ	ON	2015/08/24 21:20
S8	1	((Chad) near2 (Bacher)).INV.	US-PGPUB; USPAT	ADJ	ON	2015/08/24 21:20
S10	69	(network with forensic) with sniffers	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/08/25 15:19
S12	1	(event with action) with (textual or contextual) with target and "726".clas.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/08/25 16:28
S13	11	(event with action) with (textual or contextual) with target	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/08/25 16:29
S14	1	("9092616").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2015/08/25 22:01
S15	1	("20130298244").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2015/08/25 22:02

EAST Search History (Interference)

IPR2023-00126

CrowdStrike EX1010 Page 107

< This search history is empty >

9/ 2/ 2015 4:01:51 PM

C:\ Users\ gshehni\ Documents\ EAST\ Workspaces\ 14270069.wsp

Search Notes 	Application/Control No. 14270069	Applicant(s)/Patent Under Reexamination JAROCH ET AL.
	Examiner GHAZAL SHEHNI	Art Unit 2436

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
726	All	9/2/2015	GS

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor search (see search history printout)	9/2/2015	GS
East (see search history printout)	9/2/2015	GS
class 726 with text search	9/2/2015	GS

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

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



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/270,069	05/05/2014	Joseph Jaroch	04584.0021USU1

CONFIRMATION NO. 9580

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

PUBLICATION NOTICE



OC000000071734413

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

Publication No.US-2014-0331322-A1

Publication Date:11/06/2014

NOTICE OF PUBLICATION OF APPLICATION

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

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

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

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

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

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



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
14/270,069	05/05/2014	Joseph Jaroch	6890-103

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

CONFIRMATION NO. 9580
POA ACCEPTANCE LETTER



Date Mailed: 07/01/2014

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 06/25/2014.

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.

/masfaw/

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

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

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

Application Number	14/270,069
Filing Date	May 5, 2014
First Named Inventor	Joseph Jaroch
Title	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS
Art Unit	2414
Examiner Name	
Attorney Docket Number	04584.0021USU1

SIGNATURE of Applicant or Patent Practitioner

Signature	/Andrew T. Pouzeshi/	Date (Optional)	June 25, 2014
Name	Andrew T. Pouzeshi	Registration Number	67672
Title (if Applicant is a juristic entity)			
Applicant Name (if Applicant is a juristic entity)			

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

☐

*Total of _____ forms are submitted.

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

POWER OF ATTORNEY BY APPLICANT

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

Application Number

Filing Date

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

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

23552

OR

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

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

☒ The address associated with the above-mentioned Customer Number

OR

☐ The address associated with Customer Number:

OR

Firm or
Individual Name

Address

City

State

Zip

Country

Telephone

Email

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

WEBROOT INC.

- ☐ Inventor or Joint Inventor (title not required below)
- ☐ Legal Representative of a Deceased or Legally Incapacitated Inventor (title not required below)
- ☒ Assignee or Person to Whom the Inventor is Under an Obligation to Assign (provide signer's title if applicant is a juristic entity)
- ☐ Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is concurrently being filed with this document) (provide signer's title if applicant is a juristic entity)

SIGNATURE of Applicant for Patent

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

Signature

Date (Optional)

May 12, 2014

Name

Ryan Howe

Title

Associate General Counsel

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

☐ Total of _____ forms are submitted.

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

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

STATEMENT UNDER 37 CFR 3.73(c)Applicant/Patent Owner: Webroot Inc.Application No./Patent No.: 14/270,069Filed/Issue Date: May 5, 2014Titled: METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKSWebroot Inc., a corporation

(Name of Assignee)

(Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that, for the patent application/patent identified above, it is (choose one of options 1, 2, 3 or 4 below):

1. ☒ The assignee of the entire right, title, and interest.
2. ☐ An assignee of less than the entire right, title, and interest (check applicable box):
- ☐ The extent (by percentage) of its ownership interest is _____%. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.
- ☐ There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

3. ☐ The assignee of an undivided interest in the entirety (a complete assignment from one of the joint inventors was made). The other parties, including inventors, who together own the entire right, title, and interest are:

Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

4. ☐ The recipient, via a court proceeding or the like (e.g., bankruptcy, probate), of an undivided interest in the entirety (a complete transfer of ownership interest was made). The certified document(s) showing the transfer is attached.

The interest identified in option 1, 2 or 3 above (not option 4) is evidenced by either (choose one of options A or B below):

- A. ☒ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel 032984, Frame 0835, or for which a copy thereof is attached.
- B. ☐ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

2. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

[Page 1 of 2]

This collection of information is required by 37 CFR 3.73(b). 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 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**

STATEMENT UNDER 37 CFR 3.73(c)

3. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
 Reel _____, Frame _____, or for which a copy thereof is attached.

4. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
 Reel _____, Frame _____, or for which a copy thereof is attached.

5. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
 Reel _____, Frame _____, or for which a copy thereof is attached.

6. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
 Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☒ As required by 37 CFR 3.73(c)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/Andrew T. Pouzeshi/

June 25, 2014

Signature

Date

Andrew T. Pouzeshi

67672

Printed or Typed Name

Title or Registration 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.

Electronic Acknowledgement Receipt

EFS ID:	19404112
Application Number:	14270069
International Application Number:	
Confirmation Number:	9580
Title of Invention:	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS
First Named Inventor/Applicant Name:	Joseph Jaroch
Customer Number:	22442
Filer:	Andrew T. Pouzeshi/Jacquelyn Slate
Filer Authorized By:	Andrew T. Pouzeshi
Attorney Docket Number:	6890-103
Receipt Date:	25-JUN-2014
Filing Date:	05-MAY-2014
Time Stamp:	11:30:09
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	2014_06_25_POA_Executed_04584_0021USU1.PDF	271455 445ed71e9eefc69a8f2fade7943b8804d440799b	no	2

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:

2	Assignee showing of ownership per 37 CFR 3.73.	2014_06_25_373c_04584_002 1USU1.PDF	118138	no	3
			8332a08fecbd492a136d4ceda3b4e5b2bda a392e		

Warnings:

Information:

Total Files Size (in bytes):			389593
------------------------------	--	--	--------

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875						Application or Docket Number 14/270,069				
APPLICATION AS FILED - PART I										
(Column 1)		(Column 2)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY				
FOR	NUMBER FILED	NUMBER EXTRA	RATE(\$)	FEE(\$)		RATE(\$)	FEE(\$)			
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	70		N/A				
SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A	300		N/A				
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	360		N/A				
TOTAL CLAIMS (37 CFR 1.16(j))	20	minus 20 = *	x 40 =	0.00	OR					
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3	minus 3 = *	x 210 =	0.00						
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			0.00						
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00						
			TOTAL	730		TOTAL				
* If the difference in column 1 is less than zero, enter "0" in column 2.										
APPLICATION AS AMENDED - PART II										
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY		
AMENDMENT A		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x	=	OR	x	=
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x	=	OR	x	=
	Application Size Fee (37 CFR 1.16(s))							OR		
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY		
AMENDMENT B		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x	=	OR	x	=
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x	=	OR	x	=
	Application Size Fee (37 CFR 1.16(s))							OR		
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3. ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3". The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.										



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO	TOT CLAIMS	IND CLAIMS
14/270,069	05/05/2014	2414	800	6890-103	20	3

CONFIRMATION NO. 9580

22442
Sheridan Ross PC
1560 Broadway
Suite 1200
Denver, CO 80202

FILING RECEIPT



Date Mailed: 05/15/2014

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

Inventor(s)

Joseph Jaroch, Deer Park, IL;
Jacques Etienne Erasmus, Belper, UNITED KINGDOM;
Paul Barnes, Derby, UNITED KINGDOM;
Johannes Mayr, Linz, AUSTRIA;
Michael Leidesdorff, Niwot, CO;
Marco Giuliani, Bastia Umbra (PG), 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: None

Domestic Priority data as claimed by applicant

This appln 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 - A proper **Authorization to Permit Access to Application by Participating Offices** (PTO/SB/39 or its equivalent) has been received by the USPTO.

If Required, Foreign Filing License Granted: 05/13/2014

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 14/270,069**

Projected Publication Date: 11/06/2014

Non-Publication Request: No

Early Publication Request: No

**** SMALL ENTITY ****

Title

METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS

Preliminary Class

370

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.

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

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

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

As the below named inventor, I hereby declare that:

This declaration is directed to: ☒ The attached application, or ☐ United States application or PCT international application number _____ filed on _____.

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

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

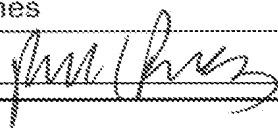
I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

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

LEGAL NAME OF INVENTOR

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

Signature: 

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

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

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

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.

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

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

As the below named inventor, I hereby declare that:

This declaration is directed to: ☒ The attached application, or
☐ United States application or PCT international application number _____
filed on _____.

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

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

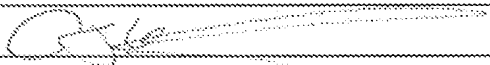
I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

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

LEGAL NAME OF INVENTOR

Inventor: Christopher Jon Williams Date (Optional): _____

Signature: 

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

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

If you need assistance in completing the form, call 1-800-PTO-8199 and select option 2.

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2905. 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 Acknowledgement Receipt

EFS ID:	18977629
Application Number:	14270069
International Application Number:	
Confirmation Number:	9580
Title of Invention:	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS
First Named Inventor/Applicant Name:	Joseph Jaroch
Customer Number:	22442
Filer:	Brent Robert Lindon/Kathy Johnston
Filer Authorized By:	Brent Robert Lindon
Attorney Docket Number:	6890-103
Receipt Date:	08-MAY-2014
Filing Date:	
Time Stamp:	13:39:54
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	Oath or Declaration filed	DEC_Barnes.pdf	941248 615f24683a5b1253f4eb572086e4a2ed8bf4338e	no	2

Warnings:

Information:

IPR2023-00126

2	Oath or Declaration filed	DEC_Williams.pdf	904361 b3f5aae051da6bfc0c86462f6320c5784ee2b7db	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			1845609		
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.					

Document code: WFEE

United States Patent and Trademark Office
Sales Receipt for Accounting Date: 05/13/2014

VVAN11	SALE	#00000027	Mailroom Dt: 05/08/2014	191970	14270069
		01 FC : 2051	70.00 DA		

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

Title of
Invention

METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO
SYSTEMS AND NETWORKS

As the below named inventor, I hereby declare that:

This declaration
is directed to:



The attached application, or



United States application or PCT international application number _____

filed on _____

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

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

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

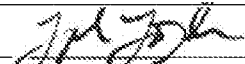
WARNING:

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

LEGAL NAME OF INVENTOR

Inventor: Joseph A. Jaroch

Date (Optional): 5/4/2014

Signature: 

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

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

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

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

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

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

As the below named inventor, I hereby declare that:

This declaration
is directed to:

☒

The attached application, or

☐

United States application or PCT international application number _____
filed on _____.

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

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

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

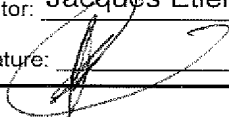
WARNING:

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

LEGAL NAME OF INVENTOR

Inventor: Jacques Etienne Erasmus

Date (Optional): 05-05-14

Signature: 

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

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

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

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

Title of
Invention

**METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO
SYSTEMS AND NETWORKS**

As the below named inventor, I hereby declare that:

This declaration
is directed to:



The attached application, or



United States application or PCT international application number _____

filed on _____

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

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

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

WARNING:

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

LEGAL NAME OF INVENTOR

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

Signature: _____

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

This collection of information is required by 35 U.S.C. 118 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

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

**DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN
APPLICATION DATA SHEET (37 CFR 1.76)**Title of
Invention**METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO
SYSTEMS AND NETWORKS**

As the below named inventor, I hereby declare that:

This declaration
is directed to:

The attached application, or



United States application or PCT international application number _____

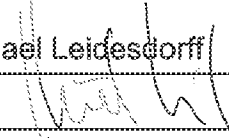
filed on _____

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

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

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

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

LEGAL NAME OF INVENTORInventor: Michael Leidesdorff Date (Optional): 5/5/14Signature: 

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

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

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

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

Title of
Invention

METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS

As the below named inventor, I hereby declare that:

This declaration
is directed to:



The attached application, or



United States application or PCT international application number _____
filed on _____

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

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

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

WARNING:

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

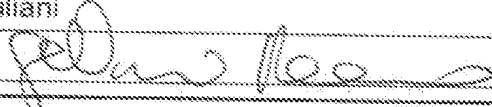
LEGAL NAME OF INVENTOR

Inventor:

Marco Giuliani

Date (Optional):

Signature:



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

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

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

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

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

As the below named inventor, I hereby declare that:

This declaration is directed to: ☒ The attached application, or
☐ United States application or PCT international application number _____
filed on _____.

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

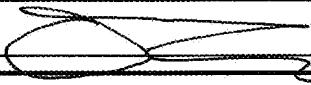
I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

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

WARNING:

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

LEGAL NAME OF INVENTOR

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

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

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

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

METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS

CROSS-REFERENCE TO RELATED APPLICATIONS

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

FIELD

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

BACKGROUND

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

 However, existing network forensic tools, such as network sniffers and packet capturing tools, passively collect information about network traffic. Such tools may be
25 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
30 devices have no ability to establish any sort of context from within the host or system that is generating the event. Therefore, devices residing at a network edge may monitor,

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

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

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

SUMMARY

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

context and a global perspective is provided for each capture event. For example, a sensor agent may provide visibility into occurrences across an environment, such as a networked environment, to ensure that an administrator is aware of any system changes and data communication in and out of computing devices residing on the network. In this
5 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.

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

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

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

In addition, data normalization takes items such as kernel filenames, usermode filenames, process objects, registry objects, and other system structures and normalizes them into a standard format which is easy more easily consumed by automated parsers.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

BRIEF DESCRIPTION OF THE DRAWINGS

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

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

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

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

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

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

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

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

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

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

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

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

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

15 DETAILED DESCRIPTION

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

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

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

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

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

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

Table 1:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Object 3, and Object 1 as illustrated. Accordingly, a global perspective 528 indicating the age of Object 2, the popularity of Object 2, the determination of Object 2, and/or additional IP/URL information of Object 2 may be provided. Similar global perspective information 532, 536 may be obtained for Object 3 and Object 1 respectfully.

5 Accordingly, an event line may be assembled utilizing the event information, contextual state, and global perspective information. In addition, the global perspective may provide additional information pertaining to an IP/URL address. For example, such information may include a categoryID of the IP/URL, a confidence of such a categoryID, a reputation, geolocation information such as which country the IP/URL is associated with, 10 and/or a threat history associated with the IP/URL.

Referring now to Figure 6, a method 600 for providing forensic visibility into a system is provided in accordance with embodiments of the present disclosure. Method 600 is in embodiments, performed by a device, such as the sensor agent 204 and/or the end recipient 220. More specifically, one or more hardware and software components 15 may be involved in performing method 600. In one embodiment, one or more of the previously described units perform one or more of the steps of method 600. The method 600 may be executed as a set of computer-executable instructions executed by a computer system and encoded or stored on a computer-readable medium. Hereinafter, the method 600 shall be explained with reference to systems, components, units, 20 software, etc. described with Figures 1-5C.

Method 600 may continuously flow in a loop, flow according to a timed event, or flow according to a change in an operating or status parameter. Method 600 is initiated at step 604 where events of a computing system 204 may be initiated. At step 608, such an event may be detected. As previously discussed, the events, which may comprise system 25 events, may be detected by one or more system filters 340 of a sensor agent 208. The sensor agent 208 may be comparatively small compared with other commercially available forensic tools and anti-malware software. This may be achieved by the sensor agent 204 being developed in a low-level language, having direct access to system resources such as the video display, disk, memory, the network(s), and without the 30 incorporation of many standard code or dynamic linked libraries to perform these functions. Memory usage may be optimized by storing data in a local database structure

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

Method 600 then proceeds to step 612 where the local aggregator and interpreter
10 344 receives events from the low level system filters 340, collecting them in batches from the queues in which they are inserted in real-time. As previously discussed, intelligent caching may be invoked to drop events which are duplicates of recent events. Further, some data normalization may be performed at step 612 to ensure consistency. Further still, caching may be implemented sparingly but in critical areas to ensure redundant
15 events are not continually reported. Method 600 then proceeds to step 616 where a contextual state may be applied by a context analyzer 348 to the event information. Accordingly, the context analyzer correlates events to objects such that an audit trail for each individual event is created. As a contextual state is established, it is cached and aggregated to be quickly queried in subsequent lookups further reducing latency and
20 improving the responsiveness of the system. Once a contextual state is applied, method 600 then proceeds to step 620 where a global perspective is applied for each event and/or each object of the event and contextual state. Accordingly, information related to the age, popularity, and determination of an object – whether it is known good, bad, or unknown is obtained. In addition, as previously mentioned, the global perspective may
25 contain information pertaining specifically to an IP/URL address. For example, the global perspective may include information relating network activity and an assessment of the reputation and category of each website and IP address as they are contacted. This data may then be normalized. Method 600 then proceeds to step 622 where an event priority may be applied to the event. As previously discussed, the event priority may be
30 obtained utilizing a rule set and applying such a rule set to aggregated event information, contextual state information, and global perspective information. Accordingly, method

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

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

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

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

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

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

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

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

Windows\file.exe would end up normalized to %windir%\file.exe, allowing rules to be created for any full path. Similar logic is utilized for paths like %appdata% which would have unique elements per-user and would be difficult to manage if not normalized. Accordingly, once the information in the event record/event line is normalized, method
5 800 may proceed to step 820 where the events may be intelligently queued. For instance, each event record/event line may be placed in a queue according to an event type. Method 800 may then end at step 828.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

10

What is claimed is:

1. A method comprising:

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

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

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

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

transmitting the assembled event line.

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

wherein the event line is transmitted to an end recipient.

3. The method of claim 1, further comprising:

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

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

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

5. The method of claim 4, further comprising:
5 determining whether a global perspective for the at least one event has been cached;
when the global perspective for the at least one event has been cached, obtaining a global perspective for the at least one event based on the cached global perspective; and
when the global perspective for the at least one event has not been cached,
10 obtaining a global perspective for the at least one event from a community database.

6. The method of claim 5, further comprising:
determining whether the cached global perspective for the at least one event has expired; and
15 when the global perspective for the at least one event has expired, obtaining a global perspective for the at least one event from a community database.

7. The method of claim 4, further comprising:
heuristically displaying information identifying the first object performing the
20 action, information identifying the action being performed, information identifying the target upon which the act is being performed, and the global perspective according to one or more of a location associated with the first object; at least one characteristic of an outbound connection associated with the first object; a dropped executable file; an age of the first object; and a number of concurrent connections associated with the first object.
25

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

9. A system for providing forensic visibility into a system, comprising:
a device including:
a communication interface;
a processor;
5 data storage; and
a sensor agent stored on the data storage that is executable by the
processor, wherein the sensor agent is operable to:
gather one or more events defining an action of a first object acting
on a target;
10 generate a contextual state for at least one of the one or more
events by correlating the at least one event to an originating object, the contextual state
including an indication of the originating object of the first object and an indication of at
least one of a device on which the first object is executed and a user associated with the
first object;
15 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;
20 assemble an event line including details associated with the at least
one event, the details including information uniquely identifying each of the first object,
the action of the first object, the target, and the originating object; and
transmit the assembled event line utilizing the communication
interface.

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

11. The system of claim 9, further comprising:
30 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.

5 12. The system of claim 8, wherein the sensor agent is further operable to:
cache the one or more events; and
asynchronously consolidate and normalize the one or more events.

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

15 14. The system of claim 13, wherein the sensor agent is further operable to:
determine whether a global perspective for the at least one event has been cached;
when the global perspective for the at least one event has been cached, obtain a
global perspective for the at least one event based on the cached global perspective; and
when the global perspective for the at least one event has not been cached, obtain
a global perspective for the at least one event from a community database.

20 15. The system of claim 14, wherein the sensor agent is further operable to:
determine whether the cached global perspective for the at least one event has
expired; and
when the global perspective for the at least one event has expired, obtain a global
25 perspective for the at least one event from a community database.

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

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

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

20 18. The system of claim 17, further comprising a global perspective
information server including:
a processor;
a communication interface;
25 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
30 information associated with one or more of the first object and the originating object, the
information including at least one of age, popularity, a determination as to whether the

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

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

5 the action of the first object, the target, and the originating object; and

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

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

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

a processor;

a communication interface; and

20 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
25 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;

30 provide the first global perspective to the device; and

provide the second global perspective to the another device.

ABSTRACT

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

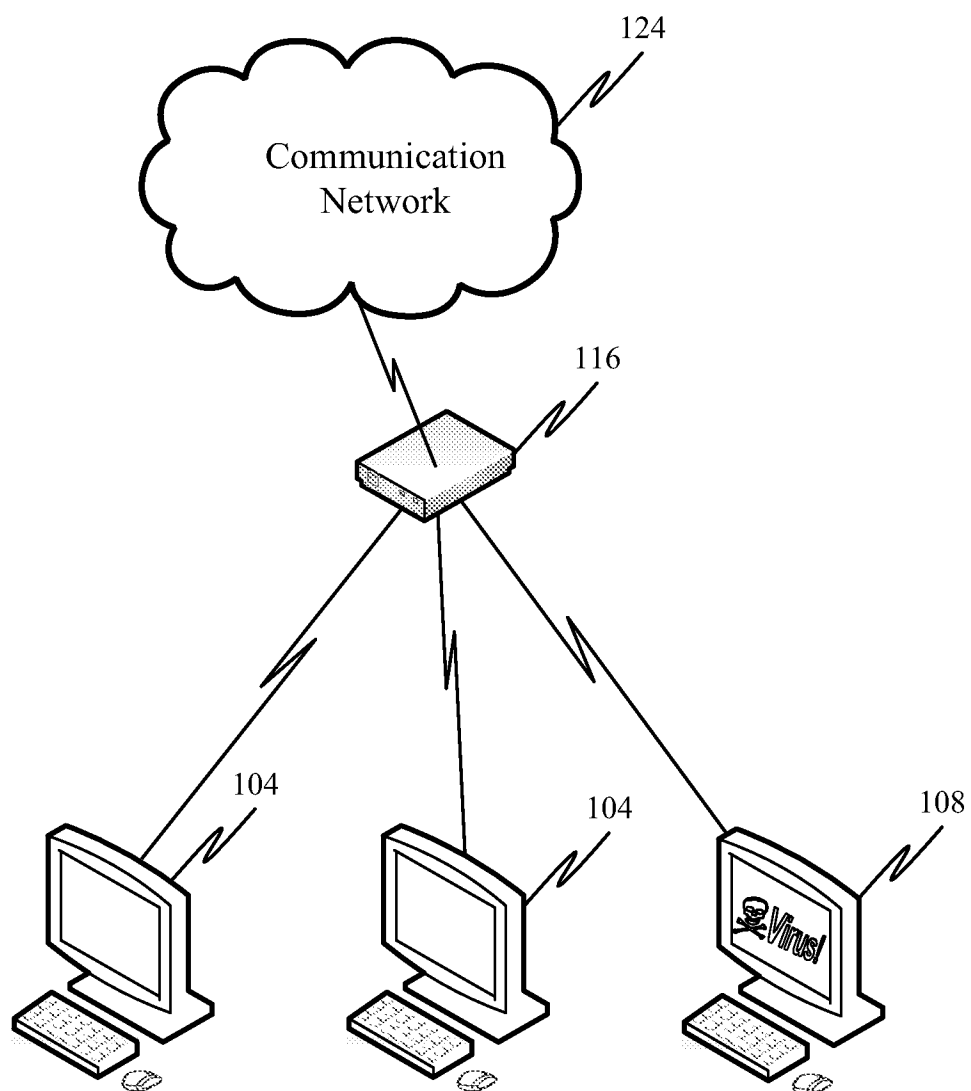


Figure 1

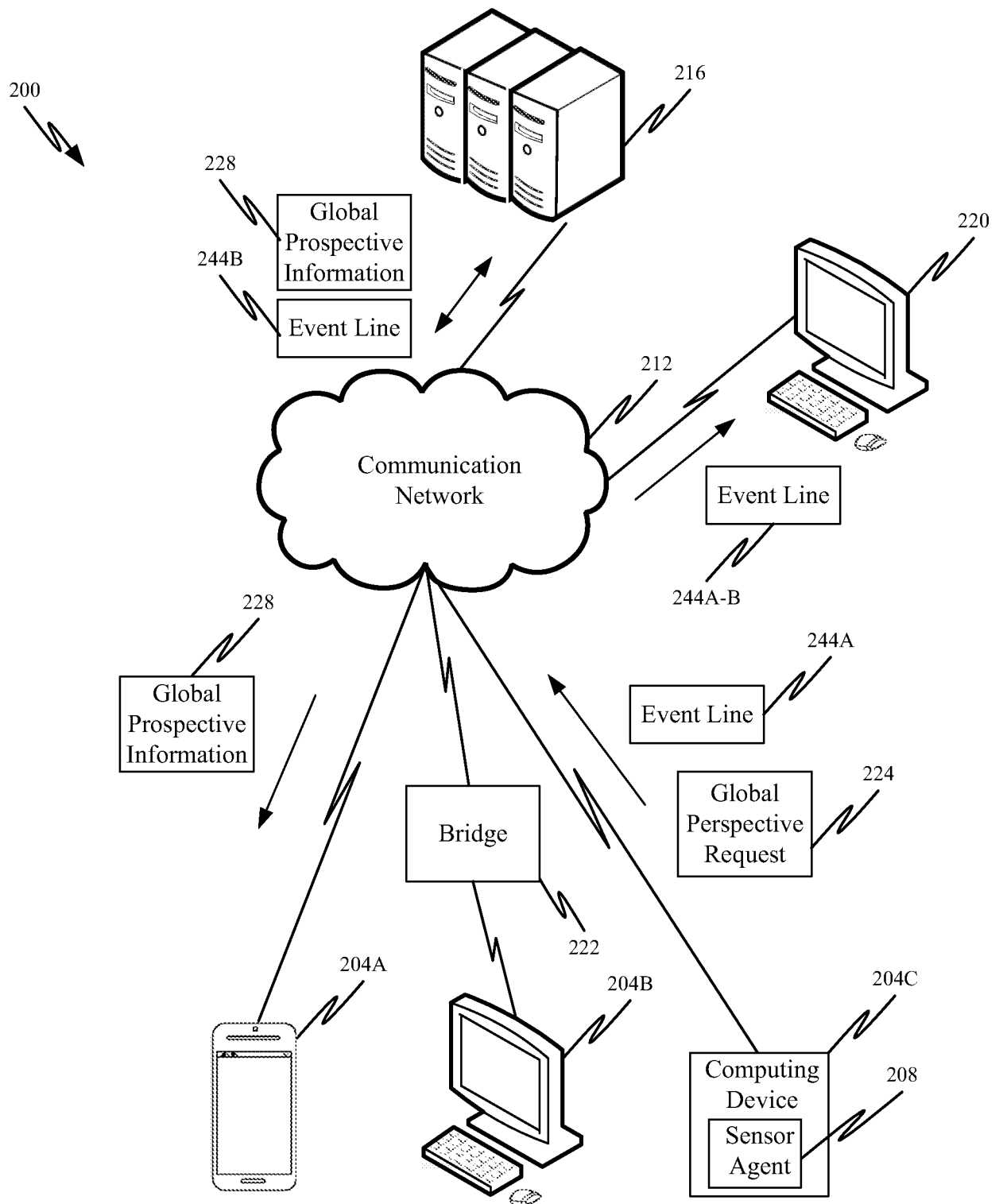


Figure 2

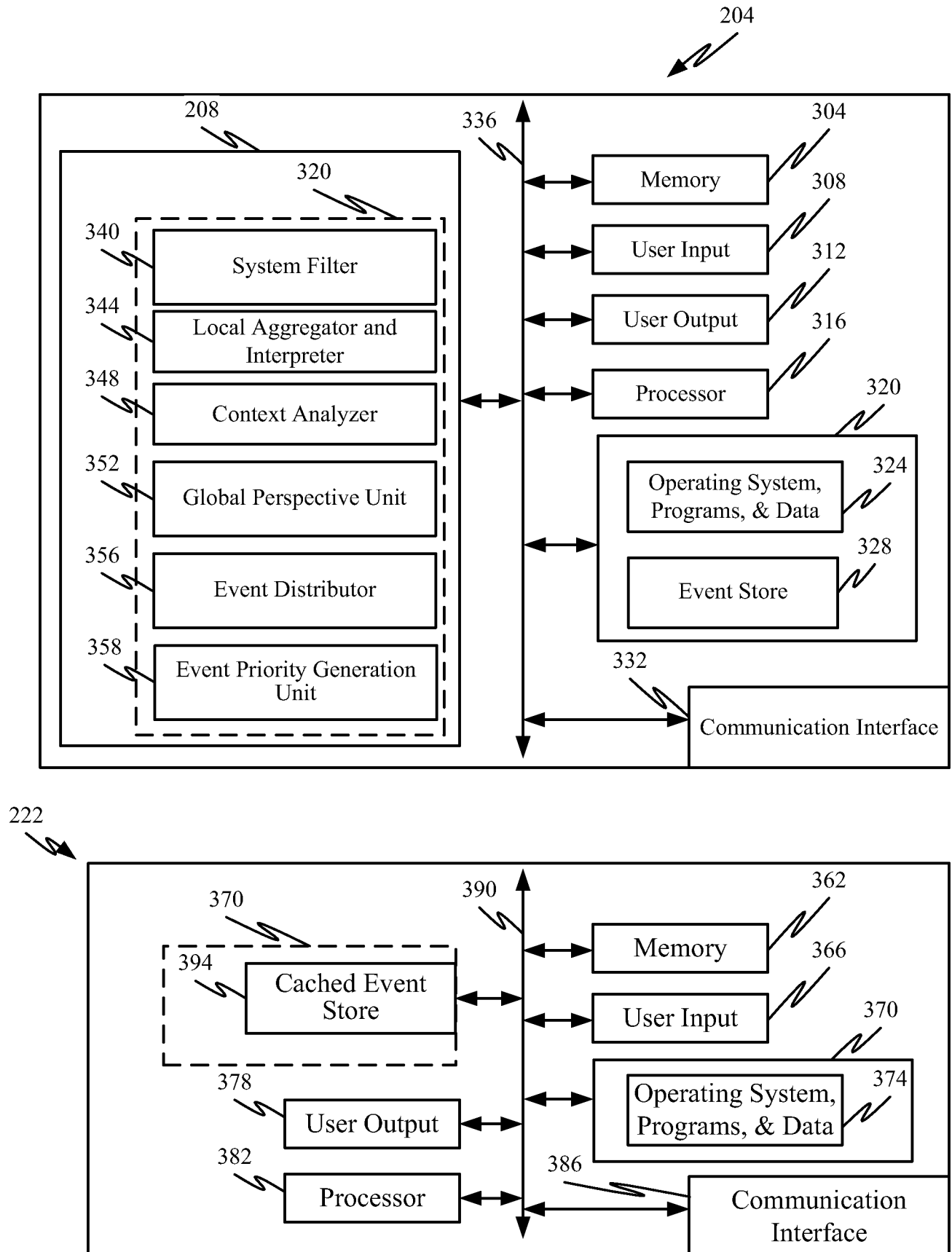


Figure 3

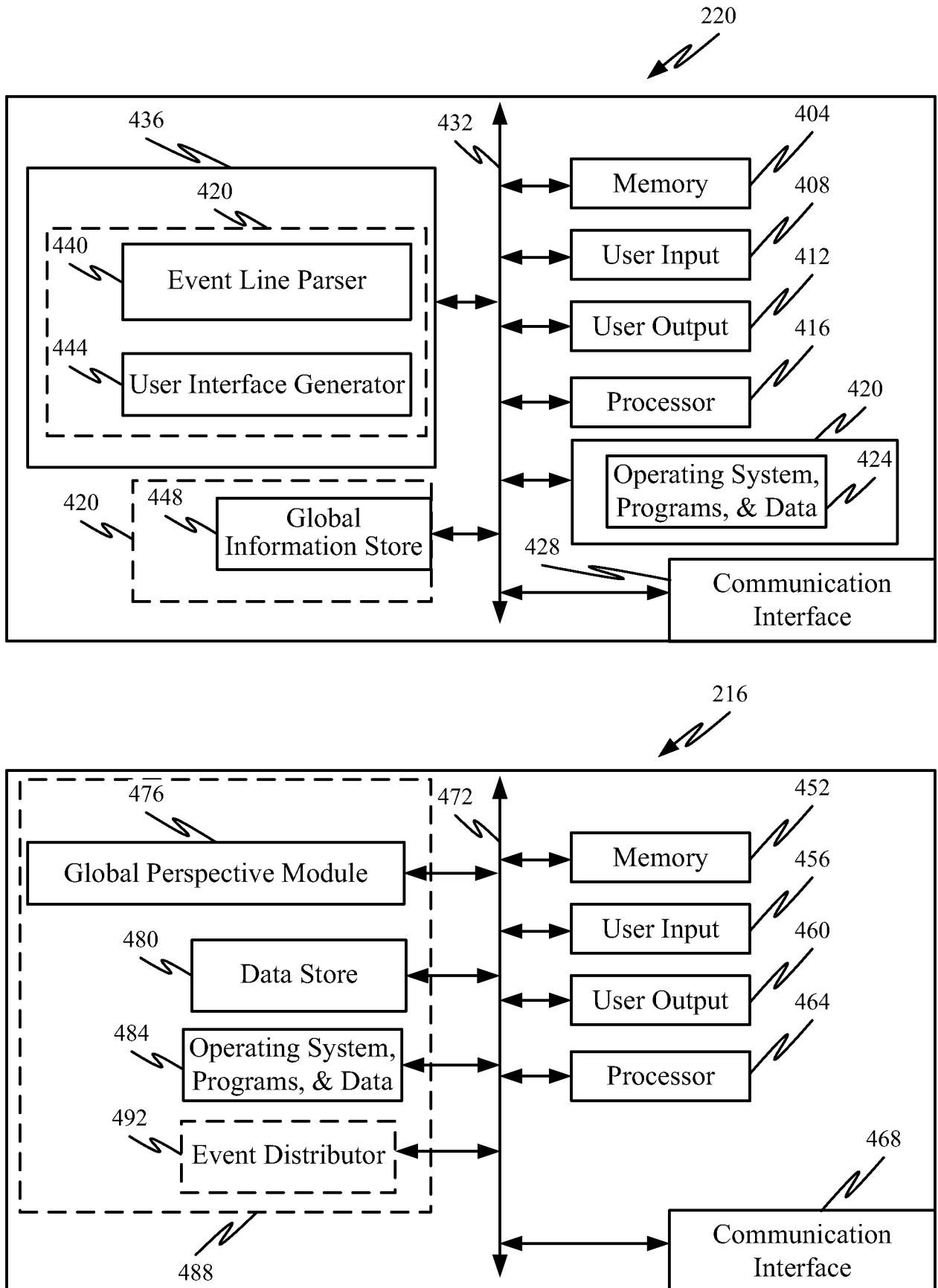


Figure 4

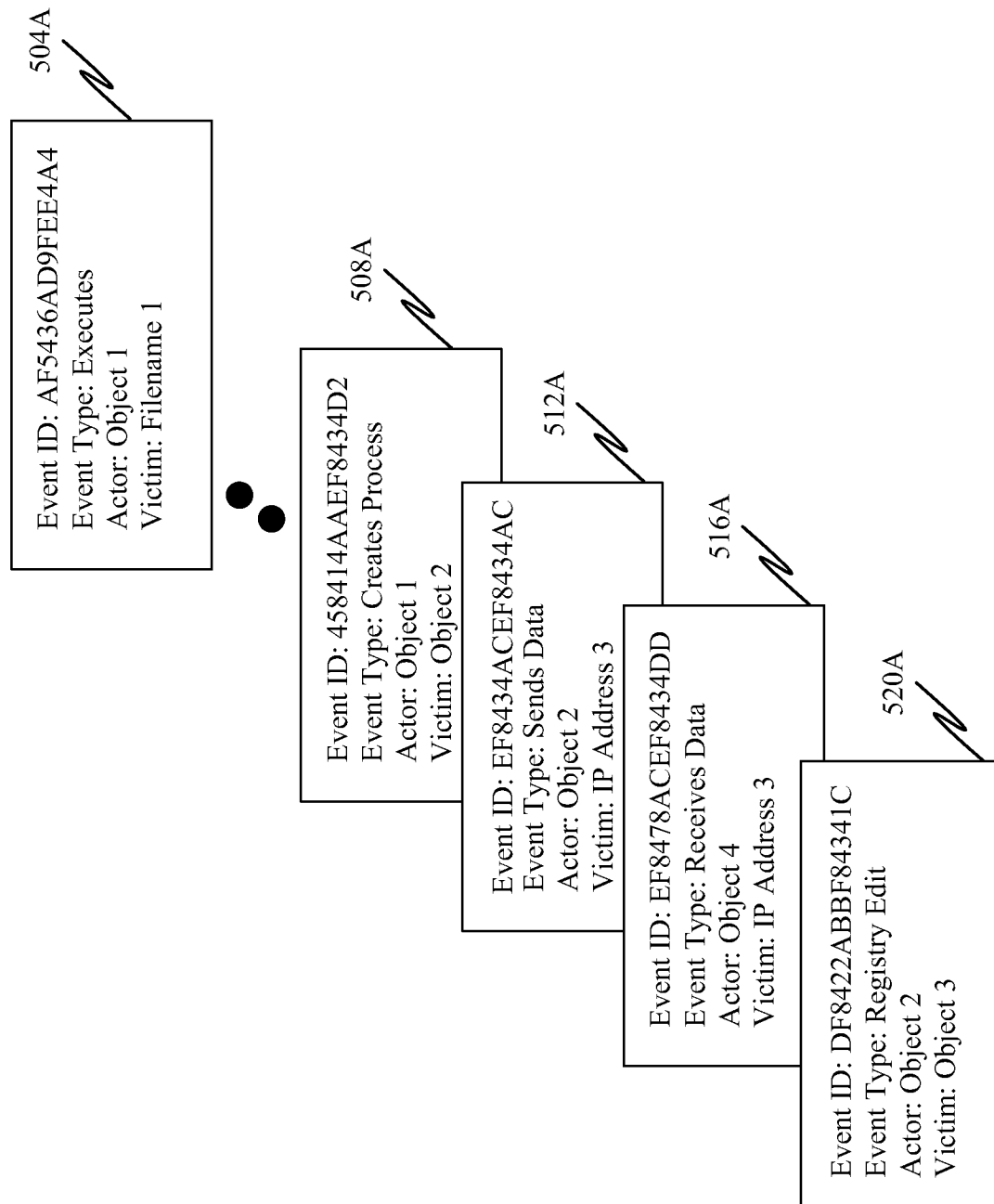


Figure 5A

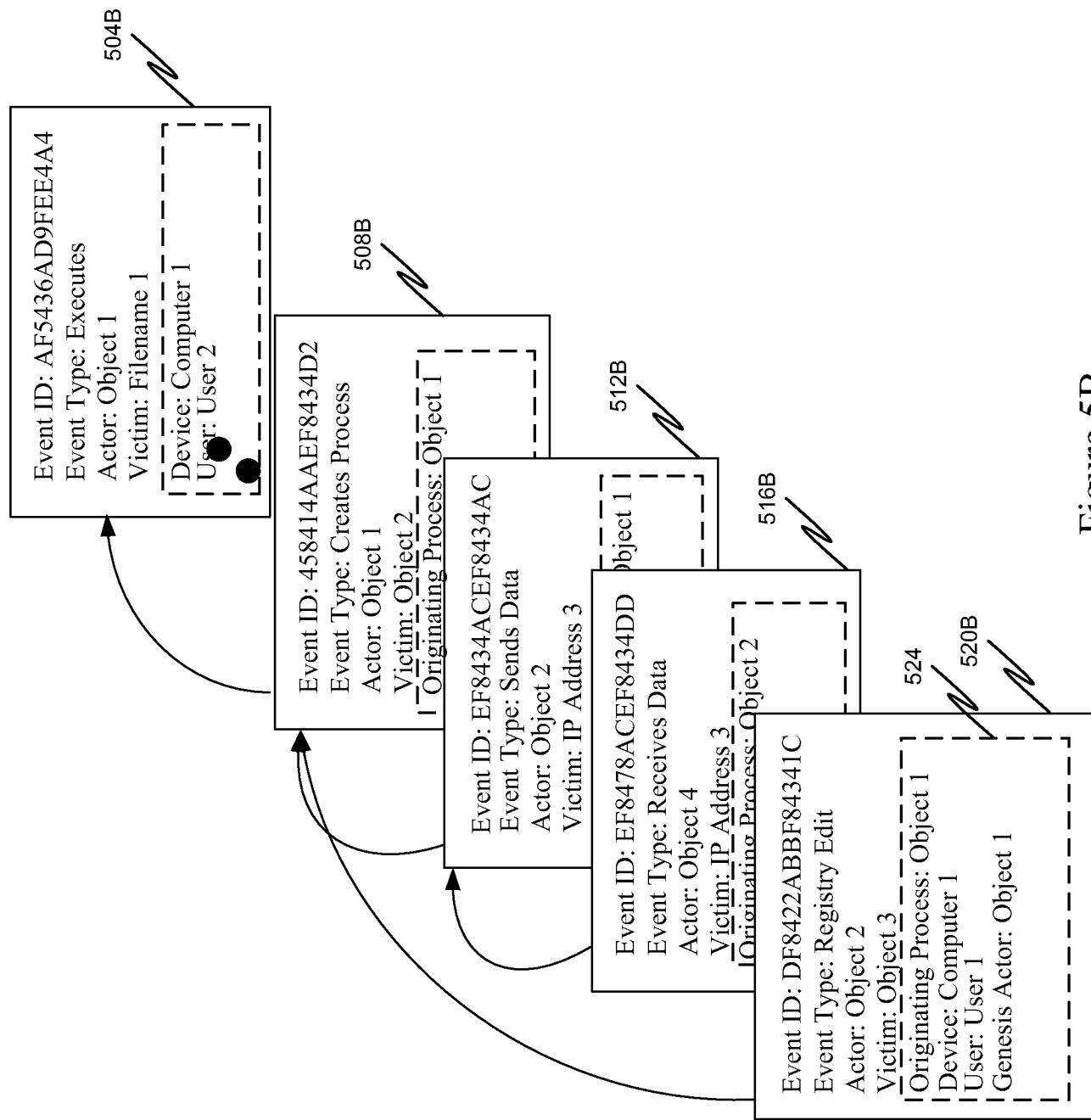


Figure 5B

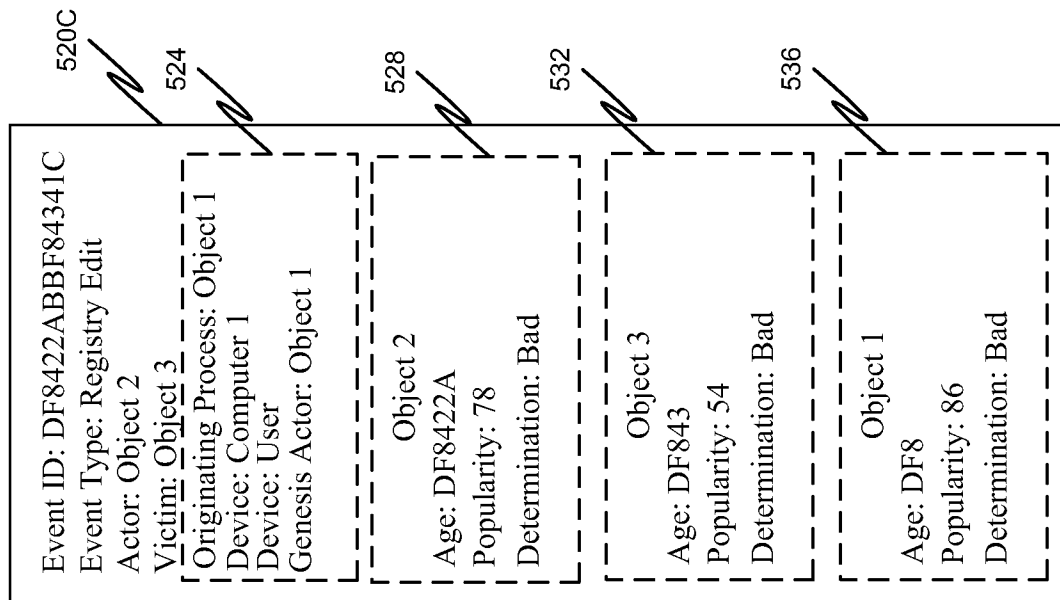


Figure 5C

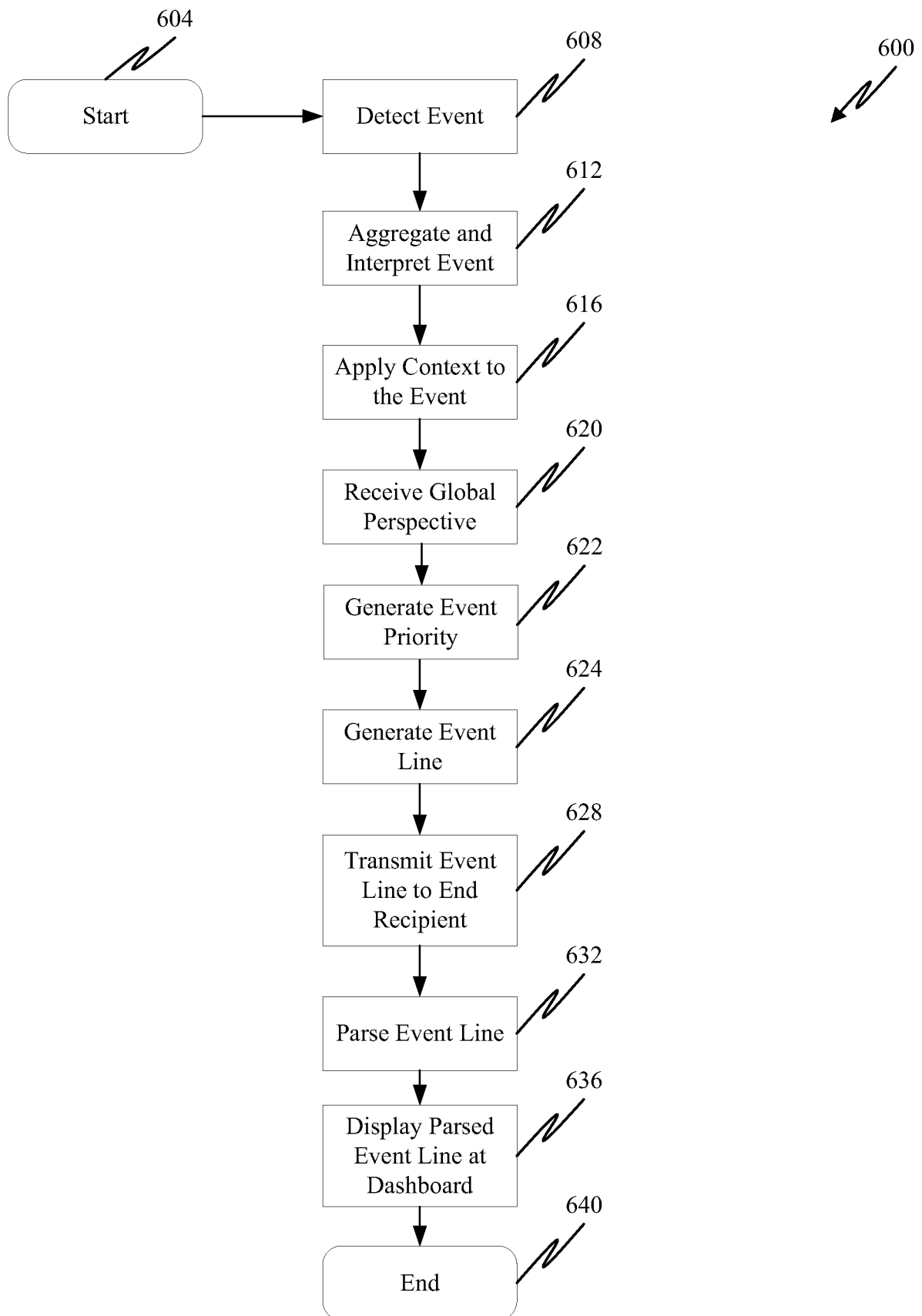


Figure 6

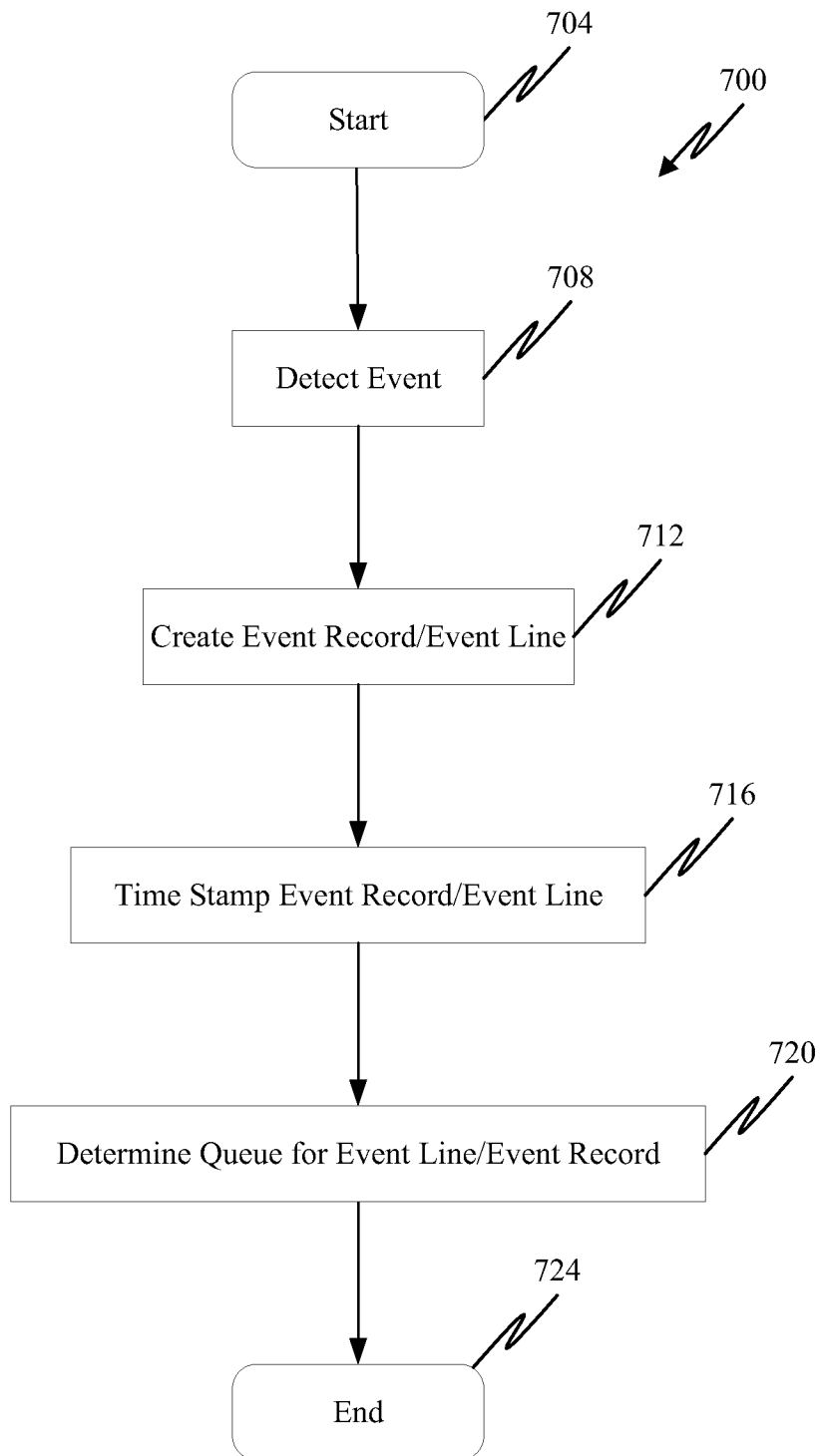


Figure 7

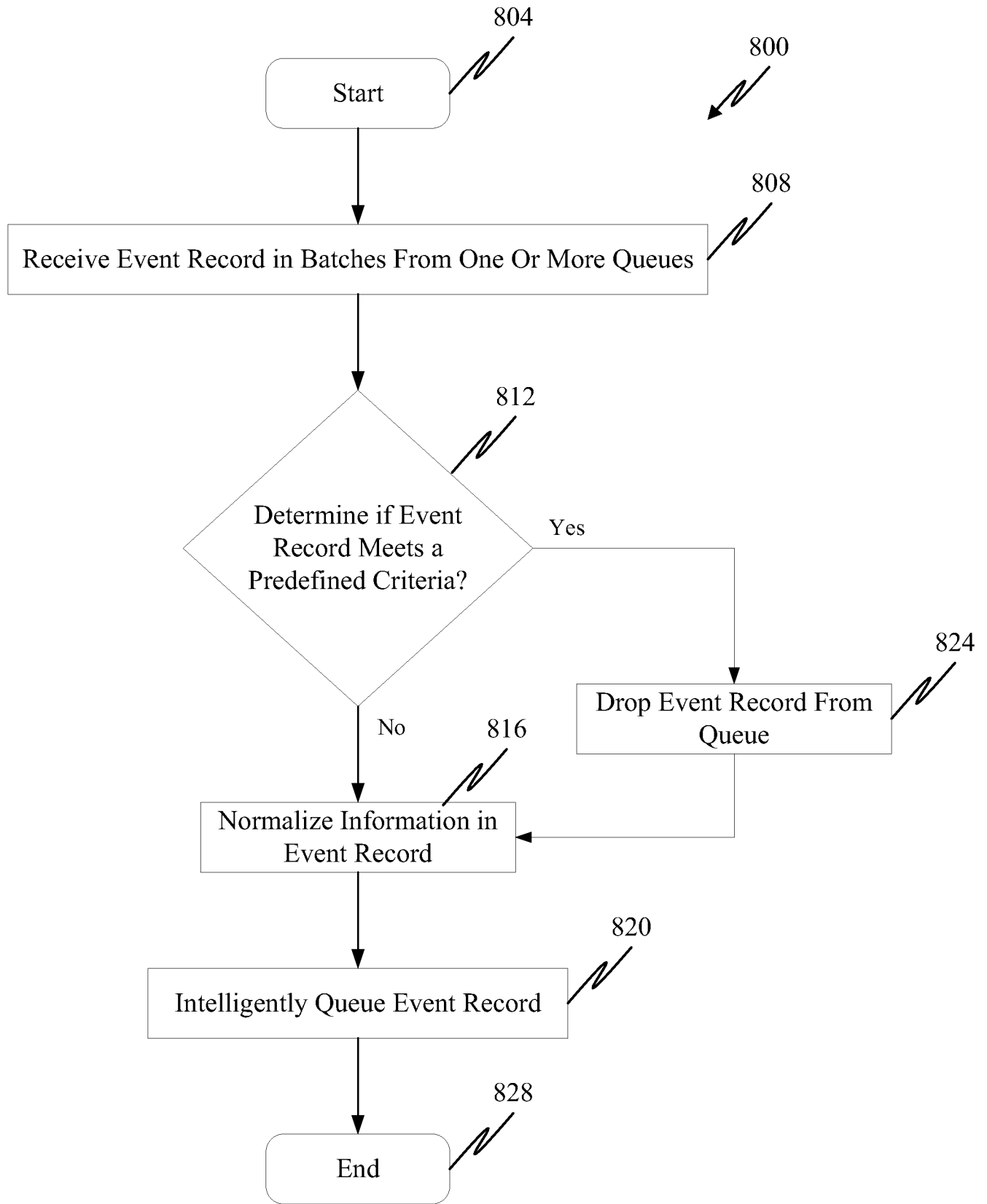


Figure 8

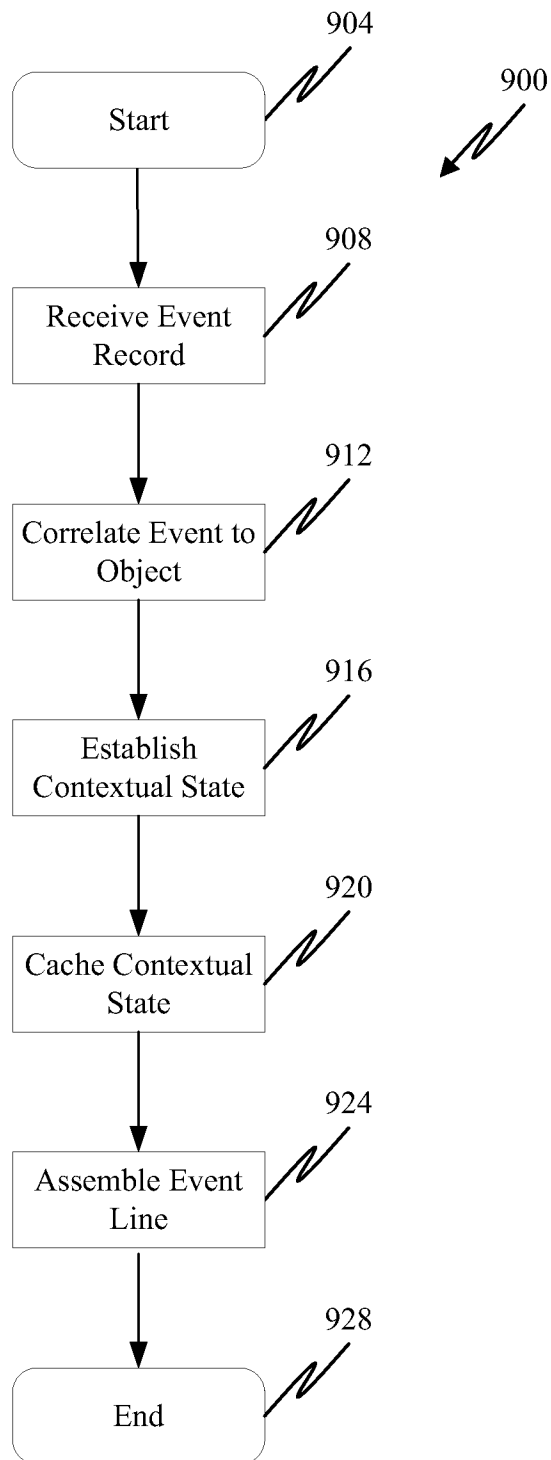


Figure 9

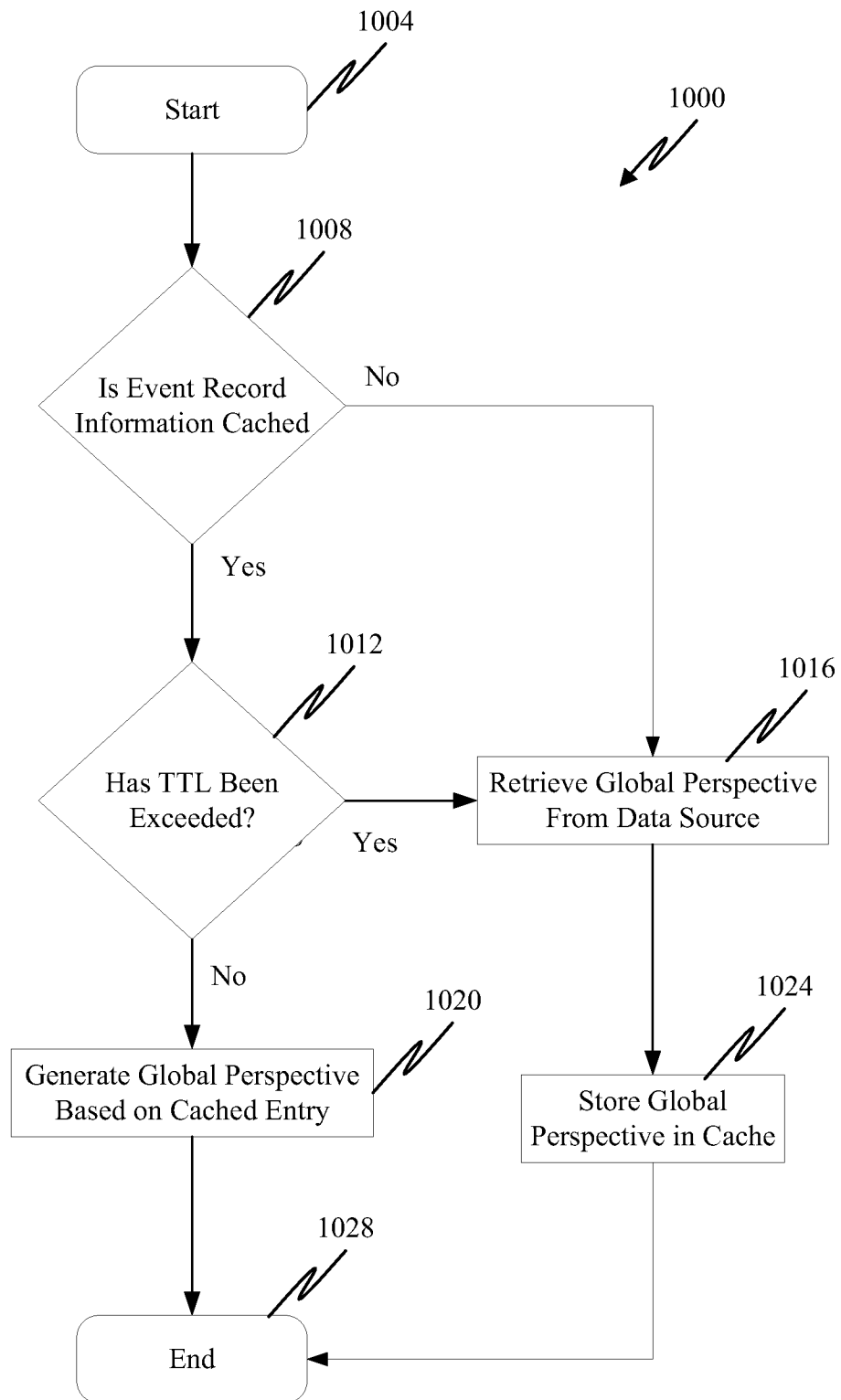


Figure 10

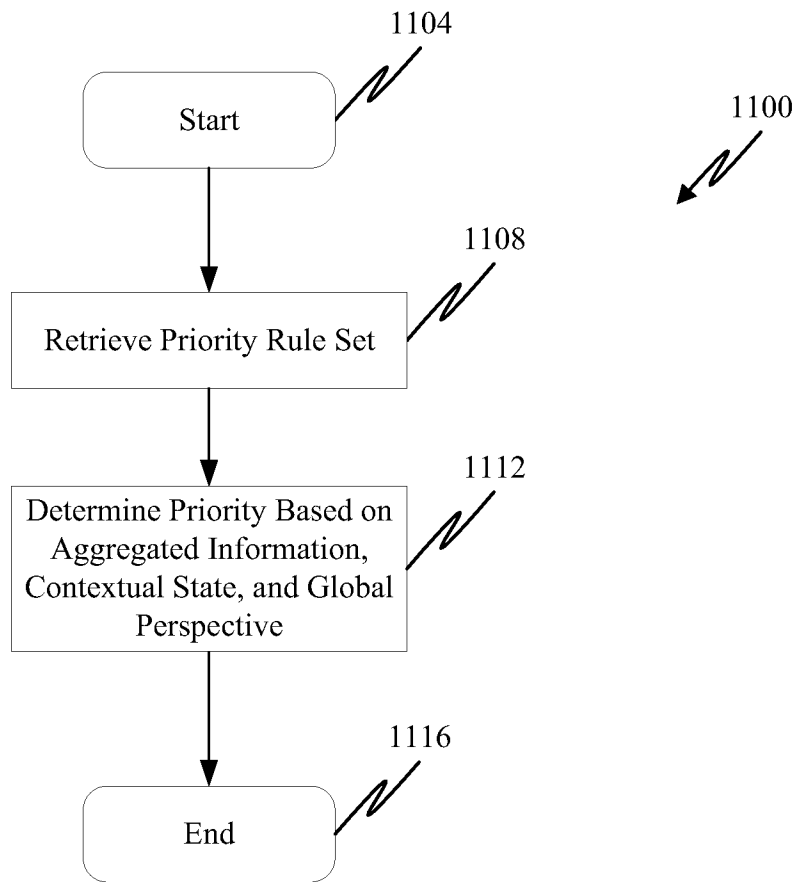


Figure 11

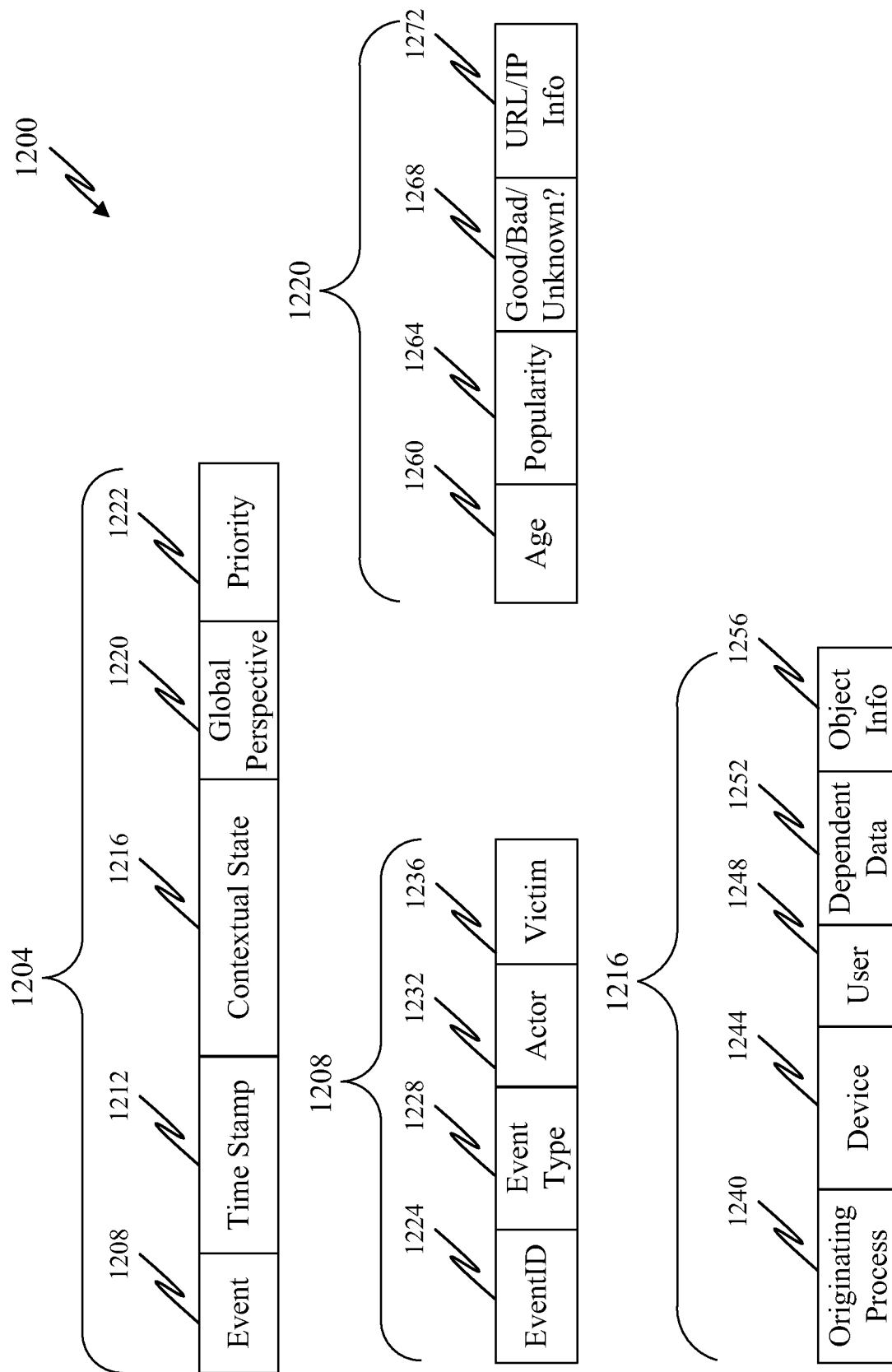


Figure 12

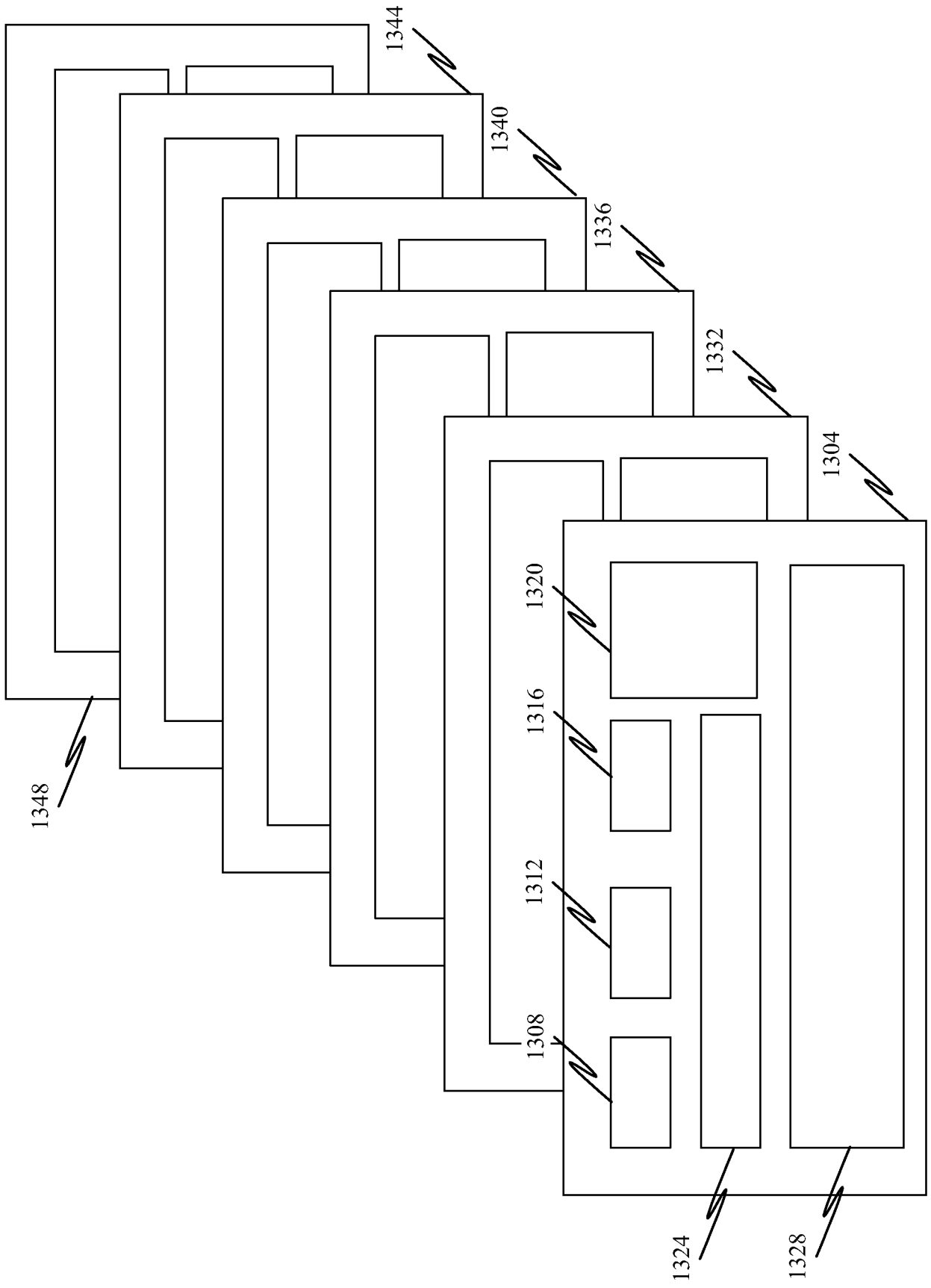


Figure 13

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	6890-103
		Application Number	
Title of Invention	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS		
The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76. This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.			

Secrecy Order 37 CFR 5.2

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

Inventor Information:

Inventor 1					Remove
Legal Name					
Prefix	Given Name	Middle Name	Family Name	Suffix	
	Joseph		Jaroch		
Residence Information (Select One) ☒ US Residency ☐ Non US Residency ☐ Active US Military Service					
City	Deer Park	State/Province	IL	Country of Residence i	US
Mailing Address of Inventor:					
Address 1		20540 N. Westpark Place			
Address 2					
City	Deer Park	State/Province	IL		
Postal Code	60010	Country i	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	Belpar	Country of Residence i	UK		
Mailing Address of Inventor:					
Address 1		8 Hillcrest			
Address 2		Overlane			
City	Belpar	State/Province			
Postal Code	DE560JF	Country i	UK		
Inventor 3					Remove
Legal Name					
Prefix	Given Name	Middle Name	Family Name	Suffix	
	Paul		Barnes		

IPR2023-00126

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	6890-103
		Application Number	
Title of Invention	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS		

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

City	Derby	Country of Residence i	UK
------	-------	------------------------	----

Mailing Address of Inventor:

Address 1	8 Wren Way		
Address 2	Mickleover		
City	Derby	State/Province	
Postal Code	DE3 OUF	Country i	UK

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	Lederergasse 31a		
Address 2			
City	Linz	State/Province	
Postal Code	4020	Country i	AT

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	8425 Firethorn Court		
Address 2			
City	Niwot	State/Province	CO
Postal Code	80503	Country i	US

Inventor 6	Remove
------------	------------------------

Legal Name

IPR2023-00126

CrowdStrike EX1010 Page 197

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	6890-103
		Application Number	
Title of Invention	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS		

Prefix	Given Name	Middle Name	Family Name	Suffix
	Marco		Giuliani	
Residence Information (Select One) ☐ US Residency ☒ Non US Residency ☐ Active US Military Service				
City	Bastia Umbra (PG)	Country of Residence i	IT	

Mailing Address of Inventor:

Address 1	Via Santa Elisabetta 21 C			
Address 2				
City	Bastia Umbra (PG)	State/Province		
Postal Code	06083	Country i	IT	
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	UK	

Mailing Address of Inventor:

Address 1	28 William Brown Square			
Address 2	Chesterfield			
City	Derbyshire	State/Province		
Postal Code	S40 2FX	Country i	UK	
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	13328 W. 87th Terrace			
Address 2				
City	Arvada	State/Province	CO	
Postal Code	80005	Country i	US	

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	6890-103
		Application Number	
Title of Invention	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS		

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

Add

Correspondence Information:

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

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

Customer Number	22442		
Email Address	srlaw@sheridanross.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	6890-103	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.

IPR2023-00126

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	6890-103
		Application Number	
Title of Invention	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS		
Please Select One:	☒ Customer Number	☐ US Patent Practitioner	☐ Limited Recognition (37 CFR 11.9)
Customer Number	22442		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this 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 blank.

Prior Application Status	Pending	Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Claims benefit of provisional	61/819470	2013-05-03
Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the Add button.			Add

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(d). When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX) the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(h)(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.			Add

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	6890-103
		Application Number	
Title of Invention	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS		

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

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.
--

Authorization to Permit Access:

☒ Authorization to Permit Access to the Instant Application by the Participating Offices
If 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 World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the instant patent application is filed access to the instant patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the instant patent application is filed to have access to the instant patent application. In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the instant patent application with respect to: 1) the instant patent application-as-filed; 2) any foreign application to which the instant patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the instant patent application; and 3) any U.S. application-as-filed from which benefit is sought in the instant patent application. In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date of filing this Authorization.

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.
--

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	6890-103
		Application Number	
Title of Invention	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS		

Applicant 1				Remove	
If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.					
Clear					
☒ Assignee		☐ Legal Representative under 35 U.S.C. 117		☐ Joint Inventor	
☐ Person to whom the inventor is obligated to assign.			☐ Person who shows sufficient proprietary interest		
If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:					
Name of the Deceased or Legally Incapacitated Inventor :					
If the Applicant is an Organization check here. ☒					
Organization Name		Webroot Inc.			
Mailing Address Information:					
Address 1		385 Interlocken Crescent, Suite 800			
Address 2					
City		Broomfield	State/Province		CO
Country ⁱ	US	Postal Code		80021	
Phone Number			Fax Number		
Email Address					
Additional Applicant Data may be generated within this form by selecting the Add button. Add					

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.			
Assignee 1			
Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication. An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.			
Remove			
If the Assignee or Non-Applicant Assignee is an Organization check here. ☐			

IPR2023-00126

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	6890-103
		Application Number	
Title of Invention	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS		

Prefix	Given Name	Middle Name	Family Name	Suffix

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1			
Address 2			
City		State/Province	
Country i		Postal Code	
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 form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications

Signature	/Brent R. Lindon/		Date (YYYY-MM-DD)	2014-05-05
First Name	Brent R.	Last Name	Lindon	Registration Number
				67424

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

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

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent 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:				
Filing Date:				
Title of Invention:	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS			
First Named Inventor/Applicant Name:	Joseph A. Jaroch			
Filer:	Brent Robert Lindon/Kathy Johnston			
Attorney Docket Number:	6890-103			
Filed as Small Entity				
Utility under 35 USC 111(a) Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Utility filing Fee (Electronic filing)	4011	1	70	70
Utility Search Fee	2111	1	300	300
Utility Examination Fee	2311	1	360	360
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

IPR2023-00126

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				730

Electronic Acknowledgement Receipt

EFS ID:	18947068
Application Number:	14270069
International Application Number:	
Confirmation Number:	9580
Title of Invention:	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS
First Named Inventor/Applicant Name:	Joseph A. Jaroch
Customer Number:	22442
Filer:	Brent Robert Lindon/Kathy Johnston
Filer Authorized By:	Brent Robert Lindon
Attorney Docket Number:	6890-103
Receipt Date:	05-MAY-2014
Filing Date:	
Time Stamp:	18:13:24
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$730
RAM confirmation Number	5693
Deposit Account	191970
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

IPR2023-00126

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 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	Oath or Declaration filed	DEC_Jaroch.pdf	225874	no	1
			c0da30c8ec487407c2a0bb57e8ed2b2d070599dc		
Warnings:					
Information:					
2	Oath or Declaration filed	DEC_Erasmus.pdf	78059	no	1
			586342bebb3ab05b7daf9210af59239311c91df0		
Warnings:					
Information:					
3	Oath or Declaration filed	DEC_Mayr.pdf	439193	no	1
			92282df25afba29fd45869a972ed74793f0150e3		
Warnings:					
Information:					
4	Oath or Declaration filed	DEC_Leidesdorff.pdf	39926	no	1
			83a36be279d65af04924f810b4d57a9a0b5d34b1		
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	Oath or Declaration filed	DEC_Giuliani.pdf	323947	no	1
			e011f4d4e87f8ebb9f84fcf8c92f94bed49fef		
Warnings:					
Information:					
6	Oath or Declaration filed	DEC_Bacher.pdf	849796	no	1
			d8c601510b0f9fb241f45c26241f5f59cd4f521		
Warnings:					
Information:					
7		Patent_Application_6890-103_Final_.pdf	173521	yes	45
			cba4a181aa1a341ac8f007757ef8e867c7e1952f		
	Multipart Description/PDF files in .zip description				
	Document Description		Start		End

IPR2023-00126

	Specification	1	37
	Claims	38	44
	Abstract	45	45

Warnings:

Information:

8	Drawings-only black and white line drawings	Figures_6890-103_Final_.pdf	82522	no	15
			b35329d3d1f632bd83c2faca7dbca41da7352dbd		

Warnings:

Information:

9	Application Data Sheet	aia0014_ADS.pdf	1566667	no	9
			549ef7da226fb9865418c12c2fe55b1cbbd0bc84		

Warnings:

Information:

10	Fee Worksheet (SB06)	fee-info.pdf	33491	no	2
			e17c8017e0f9a972e55719349b7bc63ce51a435f		

Warnings:

Information:

Total Files Size (in bytes):			3812996
------------------------------	--	--	---------

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.

SCORE Placeholder Sheet for IFW Content

Application Number: 14270069

Document Date: 05/05/2014

The presence of this form in the IFW record indicates that the following document type was received in electronic format on the date identified above. This content is stored in the SCORE database.

- Drawings – Other than Black and White Line Drawings

Since this was an electronic submission, there is no physical artifact folder, no artifact folder is recorded in PALM, and no paper documents or physical media exist. The TIFF images in the IFW record were created from the original documents that are stored in SCORE.

To access the documents in the SCORE database, refer to instructions below.

At the time of document entry (noted above):

- Examiners may access SCORE content via the eDAN interface.
- Other USPTO employees can bookmark the current SCORE URL (<http://Score.uspto.gov/ScoreAccessWeb/>).
- External customers may access SCORE content via the Public and Private PAIR interfaces.