



Online Fee Payment - Rejected payments

Account holder: CPA Computer Patent Annuities Ltd
Your account with us: 28050043

Submission date	Fee code	Application No.	User reference	Amount (EUR)	Rejection text
12.05.2021	038	14791882.5		1.330,00 +	Payment rejected: the application is definitively closed.



European Patent Office
80298 MUNICH
GERMANY

Questions about this communication ?
Contact Customer Services at www.epo.org/contact



Betten & Resch
Patent- und Rechtsanwälte PartGmbH
Postfach 10 02 51
80076 München
ALLEMAGNE

Formalities officer
Gottar, Chantal

Date
25.11.2020

Reference	Application No./Patent No. 14791882.5 - 1218 / 2992471
Applicant/Proprietor Webroot Inc.	

Acknowledgement of withdrawal of the European patent application

Receipt of the declaration of withdrawal of the European patent application on 17.11.20 is hereby acknowledged.

The proceedings are terminated as from withdrawal of the application. Any fees that have been paid but have not fallen due will be refunded.

I. FEES

- ☐ The examination fee will be refunded (OJ EPO 2016, A49):
- ☐ in full (Art. 11(a) RFees)
 - ☐ at a rate of 50% (Art. 11(b) RFees)
- ☐ The following fee(s) will be refunded:
- ☐ fee for grant including fee for publication
 - ☐ claim(s) fee
 - ☐ renewal fee(s)
 - ☐
- ☒ No fee(s) will be refunded because the requirements are not met, see in particular Art. 11(a) and (b) RFees in relation to the examination fee.

II. OTHERS

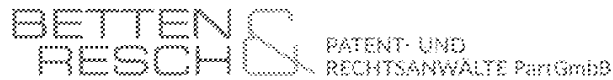
- ☒ The summons (EPO Form 2008/2008EC) dated 27.07.2020 to attend oral proceedings on 05.02.2021 is cancelled.
- ☐ The publication of the European patent application has been prevented (Rule 67(2) EPC).
- ☐ The automatic debit order ceases to be effective (point 11.1(b) AAD).
- ☐

For the Examining Division



Registered letter
EPO Form 2077N 01.20 (18/11/20)

page 1 of 1



FAX

European Patent Office
80298 Munich

November 17, 2020

European Patent Application 14791882.5
"METHOD AND APPARATUS FOR PROVIDING FORENSIC
VISIBILITY INTO SYSTEMS AND NETWORKS"
Webroot Inc.
Our File: SGR 149 WO/EP DS/MS/BO

The above application is hereby withdrawn.

Refund of all refundable fees is respectfully requested.

Dirk C. Sieckmann

Patentanwälte
European Patent Attorneys
European Trademark Attorneys
European Design Attorneys

Franz-Josef Schöninger
Dipl.-Phys.

Dr. Alexander Esslinger
Dipl.-Phys.

Dirk C. Sieckmann, LL.M.
Dipl.-Ing.

Dr. René Günther
Dipl.-Phys.

Prof. Dr. Christoph von Praun
Dipl.-Inf.

Märkte Širava, LL.M.
Dipl.-Inf.

Attila Scharfenecker
Dipl.-Phys.

Christoph Hewel
Dipl.-Ing.

Rechtsanwälte
Fachanwälte für Gewerblichen
Rechtsschutz

Alexandra Parr
Philip Reichel, LL.M.

European Patent Attorneys

Dr. Sebastian Stier
Dipl.-Phys.

Kimio Takahashi
Japanese Patent Attorney
M. Eng.

European Trademark Attorney
European Design Attorney

Dott. Isabella Peiker-Giannotti
Consulente in Marchi

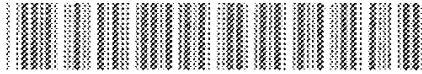
BETTEN & RESCH
Patent- und Rechtsanwälte
PartGmbH
AG München PR 1377
Maximiliansplatz 14
80333 München
Deutschland

T +49(0)89-242417-0
F +49(0)89-2607896

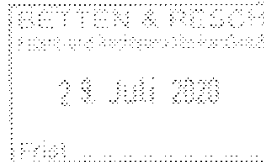
mail@bettenresch.com
www.bettenresch.com



European Patent Office
85593 MÜNCHEN
GERMANY
Tel: +49 (0) 89 2399-0
Fax: +49 (0) 89 2399-4465



Betten & Resch
Patent- und Rechtsanwälte PartGmbH
Postfach 10 02 51
80076 München
ALLEMAGNE



Formalities Officer
Name: Günter, Thomas
Tel: +49 89 2399-3239
or fax
+49 (0) 89 2399-4465

Substantive Examiner
Name: Dörner, Jörn
Tel: +49 89 2399-5470

Application No. / Patent No.
14 791 862.5 - 1218 / 2 992 471 /

Ref.

SGR 149 600/EP 023

Date

27.07.2020

Applicant
Webroot Inc.

EPA/EPO/OEB Formblatt/Form-Formulaire : EPO Form 2008, EPO Form 2908.

Empfangsbescheinigung über den Zugang des vorstehend bezeichneten Schriftstücks
Acknowledgement of receipt of the document specified above
Récépissé du document spécifié ci-dessus

Unter Bezugnahme auf die Mitteilung im ABI EPA 72010, 377 wird gebeten, die Empfangsbescheinigung mit Empfangsdatum und Unterschrift zu versehen und **umgehend** an das EPA zurückzusenden:

With reference to the Notice in OJ EPO 72010, 377, you are requested to date and sign the acknowledgement of receipt and return it to the EPO **immediately**:

Conformément au communiqué paru au JO OEB 72010, 377, vous êtes prié d'indiquer sur le récépissé la date de réception du document, de signer le récépissé et de le renvoyer **sans délai** à l'EPO :

- über die Online-Dienste des EPA (als Anlage zu EPA Form 1038) / through EPO Online Services (as annex to EPO Form 1038) / par les services en ligne de l'OEB (en tant que pièce jointe au formulaire OEB 1038).
- per Fax / by fax / par telefax (+49 (0) 89 2399-4465 or +31 (0) 70 340-3016).
- oder per Post / or by post / ou par courrier.

Empfänger am / Received on / Reçu le :

29. Juli 2020

Unterschrift / Signature:

Empfangsberechtigter/authorised recipient/le
destinataire ou la personne dûment mandatée

Rückumklebe Adresse / Return address / Adresse de retour
(Umklebung / renvoi par / renvoi par 100 / 01 / 01 / 01 / 01 / 01)

DEUTSCHLAND
80298 MÜNCHEN
Europäisches Patentamt

Rückumklebe Adresse / Return address / Adresse de retour

Registered letter

EPO Form 2008, 11.1908X

Received at the EPO on Jul 29, 2020 14:10:25. Page 1 of 1

Duration: 07.29.2020 02:09:26 PM - 07.29.2020 02:10:25 PM. This page 1 of 1 was completed at 07.29.2020 02:10:25 PM



European Patent Office
80298 MUNICH
GERMANY
Tel: +49 89 2399 0
Fax: +49 89 2399 4465



Betten & Resch
Patent- und Rechtsanwälte PartGmbH
Postfach 10 02 51
80076 München
ALLEMAGNE

Formalities Officer
Name: Gottar, Chantal
Tel: +49 89 2399 - 3203
or call
+31 (0)70 340 45 00

Substantive Examiner
Name: Dingel, Janis
Tel: +49 89 2399 - 5473

Application No. / Patent No. 14 791 882.5 - 1218 / 2 992 471 /	Ref.	Date 27.07.2020
Applicant Webroot Inc.		

EPA/EPO/OEB Formblatt/Form/Formulaire : EPO Form 2008, EPO Form 2906.

Empfangsbescheinigung über den Zugang des vorstehend bezeichneten Schriftstücks
Acknowledgement of receipt of the document specified above
Récépissé du document spécifié ci-dessus

Unter Bezugnahme auf die Mitteilung im ABI EPA 7/2010, 377 wird gebeten, die Empfangsbescheinigung mit Empfangsdatum und Unterschrift zu versehen und **umgehend** an das EPA zurückzusenden:

With reference to the Notice in OJ EPO 7/2010, 377, you are requested to date and sign the acknowledgement of receipt and return it to the EPO **immediately**:

Conformément au communiqué paru au JO OEB 7/2010, 377, vous êtes prié d'indiquer sur le récépissé la date de réception du document, de signer le récépissé et de le renvoyer **sans délai** à l'OEB :

- **über die Online-Dienste des EPA** (als Anlage zu EPA Form 1038) / **through EPO Online Services** (as annex to EPO Form 1038) / **par les services en ligne de l'OEB** (en tant que pièce jointe au formulaire OEB 1038),
- **per Fax / by fax / par telefax (+49 (0) 89 2399-4465 or +31 (0) 70 340-3016),**
- **oder per Post / or by post / ou par courrier.**

Empfangen am / Received on / Reçu le :

Unterschrift / Signature:

Empfangsberechtigter/authorised recipient/ le
destinataire ou la personne dûment mandatée

Rücksende Adresse / Return address / Adresse de retour (Umschlag / envelope / enveloppe ISO C4 / DL / C6/C5 / C6)
DEUTSCHLAND 80298 MÜNCHEN Europäisches Patentamt
Rücksende Adresse / Return address / Adresse de retour

Registered letter

EPO Form 2936 11.19CSX

Datum
Date 27.07.2020
Date

Blatt
Sheet 1
Feuille

Anmelde-Nr:
Application No: 14 791 882.5
Demande n°:

1 The examination is being carried out on the **following application documents**

Description, Pages

4-34 as published

1, 2, 2a, 2b, 3 received on 09-06-2017 with letter of 09-06-2017

Claims, Numbers

1-15 received on 26-03-2019 with letter of 26-03-2019

Drawings, Sheets

1/15-15/15 as published

2 Reference is made to the following documents; the numbering will be adhered to in the rest of the procedure.

D1 WO 2012/110501 A1 (PREVX LTD [GB]; MORRIS MELVYN [GB]; JAROCH JOSEPH [US]) 23 August 2012 (2012-08-23)

D2 US 2008/244694 A1 (NEYSTADT JOHN [IL] ET AL) 2 October 2008 (2008-10-02)

D3 WO 2006/094228 A2 (MARKMONITOR INC [US]; SHULL MARK [US]; BOHLMAN WILLIAM [US]; SHRAIM IH) 8 September 2006 (2006-09-08)

3 The applicant is summoned to oral proceedings. The objections hereafter will be discussed during the oral proceedings:

4 The present application does not meet the requirements of Article 52(1) EPC because the subject-matter of claim 1 does not involve an inventive step within the meaning of Article 56 EPC.

5 D1 deals with collecting, at a base computer, data about a computer object from each of plural remote computers on which the object or similar objects are stored and or processed.

6 D1 is regarded the closest prior art to the subject-matter of claim 1 and discloses:

***A method for providing forensic visibility into a system, comprising:
gathering one or more events defining an action of a first object acting on
a target;***

(p.21, l.28-32: "Amongst other types, the types of metadata captured and sent to the base computer 3 might be: 'Events': these define the actions or behaviours of an object acting upon another object or some other entity")

***caching the one or more events and dropping events which are duplicates
of recent events;***

("... the web server 61 just increases the count associated with that checksum in its database of the number of times that data has been seen to assist in determining the popularity of a piece of software or the frequency of the occurrence of a specific event" (D1, page 31 lines 6-16))

consolidating and normalizing the one or more events;

(Organising an event in a data structure as disclosed in D1 on page 21 line 31 - page 22 line 15 can be regarded as a form of "normalization and consolidation")

***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***

(p.21, l.28 - p.22, l.24: [...] metadata captured [...] might be: [...] 'Genesisactor': the key of an object that is not the direct Actor of an event but which is the ultimate parent of the event)

***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;***

(p.39, l.3: "The table 105 has a plurality of columns of data representing information about the objects [...]. [...] the identity of the remote computer that encountered the object, [...], the creator of the file [...]")

***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,***

(p.24, l.20-26: "In short, the agent program 10 [the] monitors objects on that computer 2 and their behaviour and communicates with the base computer 3 to send details of new objects and behaviour found on the remote computer 2 and to receive determinations of whether the objects are safe or not."; Fig. 3)

***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;***

(claim 1: "[...] at a base computer, receiving data about a computer object from each of plural remote computers [...] and apply rules and or heuristics against that data in real time to determine whether or not said object is malware and to communicate said determination to the remote computers [...])"

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

(p.29, l.18-20: "The location of the remote computer can be determined by any convenient means, such as examining the IP address")

creating an audit trail for each event to allow an end recipient to forensically track back the event, the creating comprising assembling, for each event, an event line

(p.21, line 26 - page 22, line 9: "...metadata captured and sent to the base computer 3 might be: 'Events': these define the actions or behaviours of an object acting upon another object ...")

including details associated with the event, the details including information uniquely identifying the first object as the object that triggered the event,

(idem: "The event has three principal components: the key of the object performing the act (the 'Actor')...");

the action of the first object describing an event type,

(idem: "the act being performed (the 'Event Type')")

the target upon which the action was performed,

(idem: "...the object or identity of another entity upon which the act is being performed (the 'Victim'))

a global perspective of the event, and the originating object;

(idem: "...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")

~~and transmitting the assembled event line to the end recipient.~~

- 7 The subject-matter of claim 1 therefore differs from this known method in that: transmitting the assembled event line to the end recipient.

- 8 The problem to be solved by the present invention may therefore be regarded as to provide to an end recipient an overview of all events recorded in the computer system.
- 9 The solution proposed in claim 1 of the present application cannot be considered to involve an inventive step (Articles 52(1) and 56 EPC):
- 10 In D1 all the captured data, including the metadata including the event data is stored in the databases 71-73 (D1, p. 26, lines 20-30, Fig. 3). It would be obvious for the skilled person to transmit the complete database to an end recipient, for example to allow an independent analysis by the end recipient. The skilled person would thus arrive at the solution of claim 1 without exercising an inventive step.
- 11 The subject-matter of independent claims 6 and 7 corresponds in terms of apparatus features or computer program to that of claim 1. The objections raised in respect of this latter claim, therefore, also apply to independent claims 6 and 7, which is thus not allowable under Article 56 EPC.
- 12 The additional features of the dependent claims 2-5 and 8-15 do not add anything new or inventive to the independent claims:
- 13 The additional features of claim 2 related to a community database are known from D1, Fig.1 (7), p.18, l.16: "When the community database 7 is searched for the signature of the object that was not previously known");
- 14 The additional features of claims 4, 10 and 12 are known from D1, pages 21-23 and p.18, line 4: "*If the object is still not classified locally, then details of the object are passed over the Internet 1 or other network to the base computer 3 for storing in the community database 7 and preferably for further analysis at the base computer 3*";
- 15 The additional features of claims 5, 9 and 15 related to displaying of information are known from D1, Fig. 10;
- 16 The additional features of claims 8, 9 and 14 related to global perspective information server are known from D1, Fig. 3: base computer (3).
- 17 The additional features of claim 13 are known from D1, p.21, line 26 - page 22, line 9.
- 18 The additional features of claim 3 related to obtaining event priority are not inventive over the combination of D1 with document D2. Document D2 discloses assigning a severity level to a detected incident as part of a security assessment (D2, [0015]).

- 19 The additional features of dependent claim 14 relating to the determination whether a local cache has expired are not inventive in combination with document D3, which is from the same technical field and discloses an agent for monitoring network activity and assigning trust scores to online entities (D3, Fig. 1). Trust scores are cached in a local trust cache (D3, [0086]). Cache entries may expire after a predetermined time (D3, [0093-0094]) requiring the monitoring agent to fetch updates from a trust score server.

Arguments by the applicant

- 20 The applicant argued that although D1 seems to suggest that a searchable database is maintained storing properties and activities of objects seen on remote computers (Figure 10, page 38, lines 21-28), the database does not seem to store information about events themselves.
- 21 The Examiner disagrees and points to D1, page 26, lines 20-30, Fig. 3, disclosing that metadata is stored in the database, and to page 21 line 26 - page 22 line 9, disclosing that metadata comprises event data.
- 22 The applicant further argues that D1 (for example, the searchable object database) does not provide enough information to create an audit trail, as claimed.
- 23 The Examiner disagrees and refers to the passages in D1 cited above, in particular, page 21 line 26 - page 22 line 9.



Betten & Resch
Patent- und Rechtsanwälte PartGmbH
Postfach 10 02 51
80076 München
ALLEMAGNE

Formalities Officer
Name: Gottar, Chantal
Tel: +49 89 2399 - 3203
or call
+31 (0)70 340 45 00

Substantive Examiner
Name: Dingel, Janis
Tel: +49 89 2399 - 5473

Application No. 14 791 882.5 - 1218	Ref.	Date 27.07.2020
Applicant Webroot Inc.		

Summons to attend oral proceedings pursuant to Rule 115(1) EPC

You are hereby summoned to attend oral proceedings arranged in connection with the above-mentioned European patent application.

The matters to be discussed are set out in the communication accompanying this summons (EPO Form 2906).

The oral proceedings, which will not be public, will take place before the Examining Division

on 05.02.2021 at 09:00 hrs, as a videoconference.

No changes to the date of the oral proceedings can be made, except on serious grounds (see OJ EPO 2009, 68). If you do not appear as summoned, the oral proceedings may continue without you (R. 115(2) EPC, see also OJ EPO 2008, 471).

Your attention is drawn to Rule 4 EPC, regarding the language of the oral proceedings, and to Special edition No. 3 OJ EPO 2007, L.1, concerning the filing of authorisations for company employees and lawyers acting as representatives before the EPO.

The final date for making written submissions and/or amendments (R. 116 EPC) is 05.01.2021.

You are informed that the EPO supports the following videoconferencing technologies:

- Microsoft Skype for Business Clients and SfB Room Systems
- Browser-based Web Meeting via Skype for Business WebApp
- SIP/H.323 videoconferencing systems.

The EPO provides the applicant or his representative with the opportunity to test the videoconferencing system in advance of the oral proceedings. A test call can be arranged by contacting the EPO Serviceline on Mondays to Fridays (except days on which the EPO filing offices are closed) from 7:30 to 18:00 hrs CET, by telephone (+31) (0) 70 340 44 44 or by email serviceline@epo.org. Further technical details can be found on the EPO website (www.epo.org).

Please supply the EPO as soon as possible with the following information concerning your videoconference studio:

- name of contact person with telephone number and email address to be used by the EPO for communicating the connection details
- type and name of videoconference equipment
- telephone and fax number (if any) of the studio including country and area code.

IMPORTANT:

Please inform the EPO without delay in the event that the detailed information about the videoconference connection has not been received at least ten days before the scheduled date of the oral proceedings to be held via videoconference.

Examining Division:

Chairman:
2nd Examiner:
1st Examiner:

Jeampierre, Gérald
Meis, Marc
Dingel, Janis



Annexes:

5 page/s reasons (EPO Form 2906)



European Patent Office
80298 MUNICH
GERMANY

Questions about this communication ?
Contact Customer Services at www.epo.org/contact



Betten & Resch
Patent- und Rechtsanwälte PartGmbB
Postfach 10 02 51
80076 München
ALLEMAGNE

Date
30.06.20

Reference	Application No./Patent No. 14791882.5 - 1218 / 2992471
Applicant/Proprietor Webroot Inc.	

Communication of amended entries concerning the representative (R. 143(1)(h) EPC)

As requested, for the above-mentioned European patent application / European patent the entries concerning the representative have been amended as follows:

Betten & Resch
Patent- und Rechtsanwälte PartGmbB
Postfach 10 02 51
80076 München
DE

The amendment will be recorded in the Register of European Patents.

Important note for EPO deposit account holders

If you would like to have fee refunds credited to a deposit account held with the EPO, you should ensure that you provide clear and up-to-date refund instructions to this effect, using one of the permitted electronic means of filing (see Arrangements for deposit accounts).

For the Examining Division





Acknowledgement of receipt

We hereby acknowledge receipt of the following subsequently filed document(s):

Submission number	8759047	
Application number	EP14791882.5	
Date of receipt	25 June 2020	
Receiving Office	European Patent Office, The Hague	
Your reference	EP103926-EH	
Applicant	All applicants as on file	
Documents submitted	package-data.xml epf1038.pdf (1 p.)	ep-sfd-request.xml CDAPPR-CHOR-1.pdf\EP103926.pdf (1 p.)
Submitted by	CN=Michael Heise 38571	
Method of submission	Online	
Date and time receipt generated	25 June 2020, 09:28 (CEST)	
Message Digest	4F:10:6A:7F:17:86:B5:49:36:C8:A9:FD:C9:DB:1C:77:D1:AF:E2:81	

Correction by the EPO of errors in debit instructions filed by eOLF

Errors in debit instructions filed by eOLF that are caused by the editing of Form 1038E entries or the continued use of outdated software (all forms) may be corrected automatically by the EPO, leaving the payment date unchanged (see decision T 152/82, OJ EPO 1984, 301 and point 6.3 ff ADA, Supplement to OJ EPO 10/2007).

/European Patent Office/



Letter accompanying subsequently filed items

Representative:

Grünecker Patent- und Rechtsanwälte PartG mbB
72
Leopoldstrasse 4
80802 München
Germany

Phone: +49 89 21 23 50
Fax: +49 89 22 02 87
E-mail: info@grunecker.de

80298 Munich
Germany
Tel. +49(0)89 2399-0 | Fax -4465

P.O. Box 5818
2280 HV Rijswijk
Netherlands
Tel. +31(0)70 340-2040 | Fax -3016

10958 Berlin
Germany
Tel. +49(0)30 25901-0 | Fax -840

The document(s) listed below is (are) subsequently filed documents pertaining to the following application:

Application number

14791882.5

Applicant's or representative's reference

EP103926-EH

	Description of document	Original file name	Assigned file name
1	Request for change of representative	EP103926.pdf	CDAPPR-CHOR-1.pdf

	Payment	
1	Method of payment	Not specified

Signatures

Place: **Munich**
Date: **24 June 2020**
Signed by: **Michael Heise 38571**
Association: **Grünecker Patent- und Rechtsanwälte PartG mbB**
Representative name: **Michael Heise**
Capacity: **(Representative)**

EP103926-EH

European Patent Office
Bob-van-Benthem-Platz 1
80469 München

Ihr Zeichen / Your Ref.

Unser Zeichen / Our Ref.

Datum / Date

EP103926-EHswa

June 25, 2020

European Patent Application No. 14 791 882.5
Applicant: WEBROOT INC.

We herewith withdraw from representation of the above-identified case.

Please direct any further correspondence to:

Betten & Resch
Attn: Dirk C. Sieckmann
Maximiliansplatz 14
80333 Munich
Telephone: +49 89 24 24 170
Fax: +49 89 26 07 896
E-Mail: d.sieckmann@bettenpat.com

M. Heise

MÜNCHEN

Patentanwälte

European Patent Attorneys

Thomas Schuster
Dr. Klara Goldbach
Martin Aufenanger, LL.M., MM¹
Dr. Heike Vogelsang-Wenke
Reinhard Knauer
Dietmar Kuhl
Dr. Franz-Josef Zimmer
Bettina K. Reichelt
Dr. Anton K. Pfau
Dr. Udo Weigelt, LL.M.
Rainer Bertram
Jens C. Koch, M.S. (J of PA)
Bernd Rothaemel
Thomas W. Laubenthal, LL.M.
Dr. Andreas Kayser
Dr. Jens Hammer
Dr. Thomas Eickelkamp
Dr. Peter Miltényi²
Dr. Moritz Höffe, LL.M.
Gero Maatz-Jansen
Michael Heise
Christian Meisinger
Dr. Martin Ahr
Dr. Wolfgang Neubeck
Steven M. Zeman, Ph.D.
André Nickel
Felix Kahr
Dr. Alexander Stumvoll, LL.M.
Dr. Stefano Marchini³
Dr. Thomas Kronberger
Yilin Jin
Dr. Georg Seisenberger
Dr. Olivia Nemethova, LL.M.
Dr. Rainer Plaggenborg
Victor Lopes Aguiar
Dr. Sabine Koch
Wolfram Thomas
Dr. Markus Grammel
Dr. Jegannath Korukottu⁴
Matthias Knapp

Rechtsanwälte

Attorneys-at-Law

Dr. Ulrich Blumenröder, LL.M.
Prof. Dr. Maximilian Kinkeldey, LL.M.⁵
Dr. Karsten Brandt
Anja Franke, LL.M.
Ute Stephani
Dr. Bernd Allekotte, LL.M.⁶
Dr. Elvira Bertram, LL.M.
Babett Ertle
Christine Neuhierl
Sabine Brandstätter
Cornelia Schmitt
Petra Lübke
Dr. Holger Gauss
Dr. Nicolás Schmitz
Marina Schlumberger
Kirsten Hammerstingl
Sebastian Clotten, LL.M.
Jennifer Rosenhäger, LL.M.
Mark Peters, LL.M.
Dr. Nicola Busch
Julia Bittner, LL.M.
Sebastian Ochs
Philipp Strommer
Jan Rether
Karin Lochner
Swetlana Frese
Janje Agera, LL.M.

BERLIN

Patentanwälte

European Patent Attorneys

Dr. Patrick P. Erk, M.S. (MIT)
Tino Rumpold

KÖLN

Patentanwälte

European Patent Attorneys

Dr. Martin Dropmann
Dr. Martin Bierbaum

PARIS⁷

Conseil en Propriété Industrielle

European Patent Attorney

Dr. Wolfgang Neubeck

OF COUNSEL

Patentanwälte

European Patent Attorneys

Gottfried Klitzsch

Rechtsanwälte

Attorneys-at-Law

Dr. Helmut Eichmann
Gerhard Barth

Grünecker Patent- und Rechtsanwälte PartG mbB

Leopoldstr. 4	Tel. +49 (0) 89 21 23 50	Amtsgericht: München	Deutsche Bank München
80802 München	Fax +49 (0) 89 22 02 87	Partnerschaftsregister:	SWIFT / BIC-code: DEUT DE MM
Germany	Mail info@grünecker.de	PR 1397	IBAN: DE 47 7007 0010 0175 173400

¹ auch/also: Mediator ² auch/also: Agente de la Propiedad Industrial (España) ³ auch/also: Consulente in Brevetti (Italia)
⁴ European Patent Attorney and UK Chartered Patent Attorney ⁵ Professor an der Fachhochschule für angewandtes Management
⁶ auch/also: Attorney-at-Law, New York ⁷ in Kooperation/in cooperation



Acknowledgement of receipt

We hereby acknowledge receipt of the following subsequently filed document(s):

Submission number	8570791	
Application number	EP14791882.5	
Date of receipt	27 April 2020	
Receiving Office	European Patent Office, The Hague	
Your reference	EP103926-EH	
Applicant	All applicants as on file	
Documents submitted	package-data.xml epf1038.pdf (1 p.) CLMS-HWA-1.pdf\EP103926_claims (marked).pdf (6 p.)	ep-sfd-request.xml CLMS-1.pdf\EP103926_claims (clean).pdf (6 p.) EXRE3-1.pdf\EP103926.pdf (4 p.)
Submitted by	CN=Michael Heise 38571	
Method of submission	Online	
Date and time receipt generated	27 April 2020, 13:08 (CEST)	
Message Digest	95:54:F3:B2:C2:F9:8A:65:C7:66:E2:5B:AF:7C:28:B7:F1:0D:E2:26	

Correction by the EPO of errors in debit instructions filed by eOLF

Errors in debit instructions filed by eOLF that are caused by the editing of Form 1038E entries or the continued use of outdated software (all forms) may be corrected automatically by the EPO, leaving the payment date unchanged (see decision T 152/82, OJ EPO 1984, 301 and point 6.3 ff ADA, Supplement to OJ EPO 10/2007).

/European Patent Office/

EP Application No.: 14 791 882.5
Applicant: WEBROOT INC.
Our Ref.: EP103926-EHswa
Date: April 27, 2020

New CLAIMS (marked-up copy highlighting all amendments)

1. A method comprising:

gathering one or more events (504A-520A; 1208) defining an action of a first object (1232) acting on a target (1236);

caching the one or more events and dropping events which are duplicates of recent events;

consolidating and normalizing the one or more events;

generating a contextual state (524; 1216) for at least one of the one or more consolidated and normalized events by correlating (912) 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 (1244) on which the first object is executed and a user (1248) associated with the first object;

obtaining a global perspective for the at least one event by obtaining information (228; 528-536) associated with one or more of the first object and the originating object, the information including at least one of age (1260), popularity (1264), a determination (1268) 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 (1272);

creating an audit trail for each event to allow an end recipient (220) to forensically track back the event, the creating comprising assembling (624), for each event, an event line (244A-B) including details associated with the at least one event, the details including information uniquely identifying each of the first object as the object that triggered the event, the action of the first object describing an event type, the target upon which the action was performed, a global perspective of the event, and the originating object; and

transmitting (628) the assembled event line to the end recipient.
2. The method of claim 1, wherein the information associated with the one or more of the first object and the originating object is obtained from a community database; ~~and~~

~~wherein the event line is transmitted to an end recipient (220).~~
3. The method of claim 1 or 2, further comprising:

obtaining (1112) 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 any one of claims 1 to 3, 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; and/or

further comprising:

determining (1008) 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 (1020) 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 (1016) a global perspective for the at least one event from a community database.

5. The method of claim 4, further comprising:

determining (1012) 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 (1016) a global perspective for the at least one event from a community database; and/or

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 (1260) of the first object; and a number of concurrent connections associated with the first object.

6. A computer readable storage medium comprising processor executable instructions operable to perform the method of any one of claims 1 to 5.
7. A system for providing forensic visibility into a system, comprising:

a device (204) including:

a communication interface (332);

a processor (316);

data storage (320); and

a sensor agent (208) stored on the data storage that is executable by the processor, wherein the sensor agent is operable to:

gather one or more events (504A-520A; 1208) defining an action of a first object (1232) acting on a target (1236);

cache the one or more events and drop events which are duplicates of recent events;

consolidate and normalize the one or more events;

generate a contextual state (524; 1216) for at least one of the one or more consolidated and normalized events by correlating (912) 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 (1244) on which the first object is executed and a user (1248) associated with the first object;

create an audit trail for each event to allow an end recipient (220) to forensically track back the event, assemble (624), for each event, an event line (244A-B) for the audit trail including details associated with the ~~at least one~~ event, the details including information uniquely identifying each of the first object as the object that triggered the event, the action of the first object describing an event type, the target upon which the action was performed, a global perspective of the event, and the originating object; and

transmit (628) the assembled event line to the end recipient utilizing the communication interface.

8. The system of claim 7, further comprising a global perspective information server (216) including:

a processor (464);

a communication interface (468);

data storage (488); and

a global perspective module (476), 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 (228; 528-536) associated with one or more of the first object and the originating object, the information including at least one of age (1260), popularity (1264), a determination (1268) 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 (1272);

assemble (624) 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 (628) the assembled second event line utilizing the communication interface to ~~an~~ the end recipient (220).

9. The system of claim 7 or 8, 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 (1260) of the first object; and a number of concurrent connections associated with the first object; and/or

further comprising a bridge (222) including:

a processor (382);

a communication interface (386); and

a cached event store (394), 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 (228; 528-536) associated with one or more of the first object and the originating object, the information including at least one of age (1260), popularity (1264), a determination (1268) 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 (1272);

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.

10. The system of claim 7, wherein the sensor agent is further operable to:
 - obtain a global perspective for the at least one event by obtaining information (228) associated with one or more of the first object and the originating object, the information including at least one of age (1260), popularity (1264), a determination (1268) 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 (1272);
11. The system of claim 10, wherein the at least one of the one or more events is executed by the processor.
12. The system of claim 10 or 11, further comprising:
 - a global perspective information server (216); and
 - an end recipient device (220), 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.
13. The system of any one of claims 10 to 12, wherein the at least one event includes information uniquely identifying the object performing the action, information uniquely identifying the action being performed, and information uniquely identifying the target upon which the act is being performed.
14. The system of any one of claims 10 to 13, wherein the sensor agent is one or more of:
 - further operable to:
 - determine (1008) 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 (1020) 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 (1016) a global perspective for the at least one event from a community database; or
 - further operable to:

determine (1012) 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 (1016) a global perspective for the at least one event from a community database.

15. 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 (1260) of the first object; and a number of concurrent connections associated with the first object.

EP Application No.: 14 791 882.5
Applicant: WEBROOT INC.
Our Ref.: EP103926-EHswa
Date: April 27, 2020

CLAIMS

1. A method comprising:

gathering one or more events (504A-520A; 1208) defining an action of a first object (1232) acting on a target (1236);

caching the one or more events and dropping events which are duplicates of recent events;

consolidating and normalizing the one or more events;

generating a contextual state (524; 1216) for at least one of the one or more consolidated and normalized events by correlating (912) 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 (1244) on which the first object is executed and a user (1248) associated with the first object;

obtaining a global perspective for the at least one event by obtaining information (228; 528-536) associated with one or more of the first object and the originating object, the information including at least one of age (1260), popularity (1264), a determination (1268) 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 (1272);

creating an audit trail for each event to allow an end recipient (220) to forensically track back the event, the creating comprising assembling (624), for each event, an event line (244A-B) including details associated with the event, the details including information uniquely identifying the first object as the object that triggered the event, the action of the first object describing an event type, the target upon which the action was performed, a global perspective of the event, and the originating object; and

transmitting (628) the assembled event line to the end recipient.
2. The method of claim 1, wherein the information associated with the one or more of the first object and the originating object is obtained from a community database
3. The method of claim 1 or 2, further comprising:

obtaining (1112) 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 any one of claims 1 to 3, 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; and/or

further comprising:

determining (1008) 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 (1020) 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 (1016) a global perspective for the at least one event from a community database.

5. The method of claim 4, further comprising:

determining (1012) 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 (1016) a global perspective for the at least one event from a community database; and/or

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 (1260) of the first object; and a number of concurrent connections associated with the first object.

6. A computer readable storage medium comprising processor executable instructions operable to perform the method of any one of claims 1 to 5.
7. A system for providing forensic visibility into a system, comprising:

a device (204) including:

a communication interface (332);

a processor (316);

data storage (320); and

a sensor agent (208) stored on the data storage that is executable by the processor, wherein the sensor agent is operable to:

gather one or more events (504A-520A; 1208) defining an action of a first object (1232) acting on a target (1236);

cache the one or more events and drop events which are duplicates of recent events;

consolidate and normalize the one or more events;

generate a contextual state (524; 1216) for at least one of the one or more consolidated and normalized events by correlating (912) 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 (1244) on which the first object is executed and a user (1248) associated with the first object;

create an audit trail for each event to allow an end recipient (220) to forensically track back the event, assemble (624), for each event, an event line (244A-B) for the audit trail including details associated with the event, the details including information uniquely identifying each of the first object as the object that triggered the event, the action of the first object describing an event type, the target upon which the action was performed, a global perspective of the event, and the originating object; and

transmit (628) the assembled event line to the end recipient utilizing the communication interface.

8. The system of claim 7, further comprising a global perspective information server (216) including:

a processor (464);

a communication interface (468);

data storage (488); and

a global perspective module (476), 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 (228; 528-536) associated with one or more of the first object and the originating object, the information including at least one of age (1260), popularity (1264), a determination (1268) 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 (1272);

assemble (624) 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 (628) the assembled second event line utilizing the communication interface to the end recipient (220).

9. The system of claim 7 or 8, 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 (1260) of the first object; and a number of concurrent connections associated with the first object; and/or

further comprising a bridge (222) including:

a processor (382);

a communication interface (386); and

a cached event store (394), 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 (228; 528-536) associated with one or more of the first object and the originating object, the information including at least one of age (1260), popularity (1264), a determination (1268) 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 (1272);

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.

10. The system of claim 7, wherein the sensor agent is further operable to:
 - obtain a global perspective for the at least one event by obtaining information (228) associated with one or more of the first object and the originating object, the information including at least one of age (1260), popularity (1264), a determination (1268) 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 (1272).
11. The system of claim 10, wherein the at least one of the one or more events is executed by the processor.
12. The system of claim 10 or 11, further comprising:
 - a global perspective information server (216); and
 - an end recipient device (220), 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.
13. The system of any one of claims 10 to 12, wherein the at least one event includes information uniquely identifying the object performing the action, information uniquely identifying the action being performed, and information uniquely identifying the target upon which the act is being performed.
14. The system of any one of claims 10 to 13, wherein the sensor agent is one or more of:
 - further operable to:
 - determine (1008) 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 (1020) 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 (1016) a global perspective for the at least one event from a community database; or
 - further operable to:

determine (1012) 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 (1016) a global perspective for the at least one event from a community database.

15. 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 (1260) of the first object; and a number of concurrent connections associated with the first object.



Letter accompanying subsequently filed items

Representative:

Grünecker Patent- und Rechtsanwälte PartG mbB
72
Leopoldstrasse 4
80802 München
Germany

Phone: +49 89 21 23 50
Fax: +49 89 22 02 87
E-mail: info@grunecker.de

80298 Munich
Germany
Tel. +49(0)89 2399-0 | Fax -4465

P.O. Box 5818
2280 HV Rijswijk
Netherlands
Tel. +31(0)70 340-2040 | Fax -3016

10958 Berlin
Germany
Tel. +49(0)30 25901-0 | Fax -840

The document(s) listed below is (are) subsequently filed documents pertaining to the following application:

Application number

14791882.5

Applicant's or representative's reference

EP103926-EH

	Description of document	Original file name	Assigned file name
1	Amended claims (clean copy)	EP103926_claims (clean).pdf	CLMS-1.pdf
2	Amended claims with annotations	EP103926_claims (marked).pdf	CLMS-HWA-1.pdf
3	Reply to examination report	EP103926.pdf	EXRE3-1.pdf

	Payment	
1	Method of payment	Not specified

Signatures

Place: **Munich**
Date: **27 April 2020**
Signed by: **Michael Heise 38571**
Association: **Grünecker Patent- und Rechtsanwälte PartG mbB**
Representative name: **Michael Heise**
Capacity: **(Representative)**

EP103926-EH

European Patent Office
Bob-van-Benthem-Platz 1
80469 München

Ihr Zeichen / Your Ref.

Unser Zeichen / Our Ref.

Datum / Date

EP103926-EHswa

April 27, 2020

European Patent Application No. 14 791 882.5
Applicant: WEBROOT INC.

In response to the Official Communication pursuant to Article 94(3) EPC dated
October 17, 2019:

Submitted herewith are:

- new claims 1 to 15 to replace all claims presently on file.

Also enclosed is a marked-up version of the new claim set, highlighting all claim amendments.

The claims have been amended in order to overcome all objections raised in the above-mentioned Official Communication.

I. Amendments

New independent claim 1 is based on previously submitted claim 1 and further defines creating an audit trail for each event. This amendment can be derived from the application as originally filed, including page 4, lines 13-27; page 10, line 33 to page 11, line 11; page 17, lines 3-15; and page 25, lines 9-21.

Grünecker Patent- und Rechtsanwälte PartG mbB

Leopoldstr. 4	Tel. +49 (0) 89 21 23 50	Amtsgericht: München	Deutsche Bank München
80802 München	Fax +49 (0) 89 22 02 87	Partnerschaftsregister:	SWIFT / BIC-code: DEUT DE MM
Germany	Mail info@grunecker.de	PR 1397	IBAN: DE47 7007 0010 173400

¹ auch/also: Mediator ² auch/also: Agente de la Propiedad Industrial (España) ³ auch/also: Consulente in Brevetti (Italia)

⁴ European Patent Attorney and UK Chartered Patent Attorney ⁵ Professor an der Fachhochschule für angewandtes Management

⁶ auch/also: Attorney-at-Law, New York ⁷ in Kooperation/in cooperation

MÜNCHEN

Patentanwälte

European Patent Attorneys

Thomas Schuster
Dr. Klara Goldbach
Martin Aufenanger, LL.M., MM¹
Dr. Heike Vogelsang-Wenke
Reinhard Knauer
Dietmar Kuhl
Dr. Franz-Josef Zimmer
Bettina K. Reichelt
Dr. Anton K. Pfau
Dr. Udo Weigelt, LL.M.
Rainer Bertram
Jens C. Koch, M.S. (J of PA)
Bernd Rothaemel
Thomas W. Laubenthal, LL.M.
Dr. Andreas Kayser
Dr. Jens Hammer
Dr. Thomas Eickelkamp
Dr. Peter Miltényi²
Dr. Moritz Höffe, LL.M.
Gero Maatz-Jansen
Michael Heise
Christian Meisinger
Dr. Martin Ahr
Dr. Wolfgang Neubeck
Steven M. Zeman, Ph.D.
André Nickel
Felix Kahr
Dr. Alexander Stumvoll, LL.M.
Dr. Stefano Marchini³
Dr. Thomas Kronberger
Yilin Jin
Dr. Georg Seisenberger
Dr. Olivia Nemethova, LL.M.
Dr. Rainer Plaggenborg
Victor Lopes Aguiar
Dr. Sabine Koch
Wolfram Thomas
Dr. Markus Grammel
Dr. Jeggannath Korukottu⁴
Matthias Knapp

Rechtsanwälte

Attorneys-at-Law

Dr. Ulrich Blumenröder, LL.M.
Prof. Dr. Maximilian Kinkeldey, LL.M.⁵
Dr. Karsten Brandt
Anja Franke, LL.M.
Ute Stephani
Dr. Bernd Allekotte, LL.M.⁶
Dr. Elvira Bertram, LL.M.
Babett Ertle
Christine Neuhiel
Sabine Brandstätter
Cornelia Schmitt
Petra Lübke
Dr. Holger Gauss
Dr. Nicolás Schmitz
Marina Schlumberger
Kirsten Hammerstingl
Sebastian Clotten, LL.M.
Jennifer Rosenhäger, LL.M.
Mark Peters, LL.M.
Dr. Nicola Busch
Julia Bittner, LL.M.
Sebastian Ochs
Philipp Strommer
Jan Rether
Karin Lochner
Swetlana Frese
Janette Agena, LL.M.

BERLIN

Patentanwälte

European Patent Attorneys

Dr. Patrick P. Erk, M.S. (MIT)
Tino Rumpold

KÖLN

Patentanwälte

European Patent Attorneys

Dr. Martin Drophmann
Dr. Martin Bierbaum

PARIS⁷

Conseil en Propriété Industrielle

European Patent Attorney

Dr. Wolfgang Neubeck

OF COUNSEL

Patentanwälte

European Patent Attorneys

Gottfried Klitzsch

Rechtsanwälte

Attorneys-at-Law

Dr. Helmut Eichmann
Gerhard Barth

New dependent claims 2 to 5 are identical to previously submitted claims 2 to 5, respectively, some changes to conform to new independent claim 1 without changing the additional feature and subject matter of the respective claims.

New claim 6 corresponds to previously submitted claim 6.

New independent claim 7 is based on previously submitted claim 7 and has been amended in the same manner as corresponding claim 1.

New dependent claims 8 to 15 are identical to previously submitted claims 8 to 15, respectively, some changes to conform to new independent claim 7 without changing the additional feature and subject matter of the respective claims.

Accordingly, the claims do not introduce subject matter extending beyond the content of the application as originally filed and fulfill the requirements of Article 123(2) EPC.

II. Patentability

The Examining Division's arguments and analysis concerning the cited prior art documents are highly appreciated and have been carefully considered and taken into account by the Applicant. However, in regard to the new claims, the Examining Division is kindly requested to consider the following arguments from the Applicant understood to lead to the conclusion that the claimed subject matter is novel and involves an inventive step over the available prior art.

In particular, it is respectfully submitted by the Applicant that although D1 seems to suggest that a searchable database is maintained storing properties and activities of objects seen on remote computers (Figure 10, page 38, lines 21-28), the database does not seem to store information about events themselves. D1 relates to providing protection against malware and for classifying a computer object as malware. D1 maintains the database and collects object information from a plurality of remote computers to help identify malware in all of the remote computers.

The claimed subject matter, for a given event, generates a contextual state, obtains a global perspective, and creates an audit trail for the event to allow an end user (for

example, an administrator) to forensically track back the event. The information collected in D1 (for example, the searchable object database) does not provide enough information to create an audit trail, as claimed. Creating the audit trail in the claimed subject matter includes assembling an event line including details associated with the event, including information uniquely identifying the object that triggered the event, the action of the object (the event type), the target of the event, a global perspective of the event, and an originating object. While D1 can help provide protection against malware and classify a computer object as malware, D1 does not teach or suggest all of the steps of new claim 1, discussed above.

In view of the aforementioned distinguishing features, the claimed subject matter is considered to be novel within the meaning of Article 54 EPC.

Similarly, it is respectfully pointed out by the Applicant that that these distinguishing features are also not disclosed or suggested by the remaining cited documents D2 and D3.

In addition, it is respectfully submitted by the Applicant that creating an audit trail for an event that allows an end user to forensically track back the event, provides end-to-end forensic visibility of every event within a system and/or within a network.

Since neither D1 nor the remaining prior art disclose or suggest the aforementioned distinguishing features, the claimed subject matter does not arise from the available prior art in an obvious manner, but involves an inventive step within the meaning of Article 56 EPC.

III. Summary

As the new claims submitted herewith are considered to overcome all objections raised in the above mentioned Official Communication, the Examining Division is kindly requested to propose grant.

Should the Examining Division have further objections against the present application, it is kindly and respectfully requested that the proceedings be continued in writing by issuing a further examination report.

As a measure of precaution only, the request for oral proceedings is maintained.

M. Heise

Encl.

New claims 1 to 15 (clean and marked-up copies)



European Patent Office
80298 MUNICH
GERMANY

Questions about this communication ?
Contact Customer Services at www.epo.org/contact



Grünecker Patent- und Rechtsanwälte
PartG mbB
Leopoldstraße 4
80802 München
ALLEMAGNE

Date
05.03.20

Reference EP103926EHjet	Application No./Patent No. 14791882.5 - 1218 / 2992471
Applicant/Proprietor Webroot Inc.	

Extension of time limit pursuant to Rule 132(2) EPC

Examination procedure

With reference to your request, the time limit for replying to the communication pursuant to Article 94(3) EPC dated 17.10.19 has been extended

by 2 months

to a total of 6 months

from the date of notification of the above-mentioned communication.

Please note: To the extent that your request exceeded the above extension, your request has been refused.

Note

The granting of extensions to time limits is governed by the Implementing Regulations to the EPC and the Guidelines for Examination in the EPO, E-VIII, 1.6. A request for extension, which would result in the total period set exceeding six months, must be reasoned and supported by evidence.

If no reply to the communication is received in due time, the European patent application will be deemed to be withdrawn (Art. 94(4) EPC).

Important information in case of a PACE request

If a PACE request has been validly filed for the application, the applicant is herewith informed that with the grant of the request for extension of time limit the application is removed from the PACE programme. A second PACE request for that application during the same stage of the procedure will not be processed (see OJ EPO 2015, A93, point 4).

For the Examining Division

European Patent Office
Bob-van-Bentham-Platz 1
80469 München

EPO - Munich
102

26 Feb. 2020

Ihr Zeichen / Your Ref.

Unser Zeichen / Our Ref.

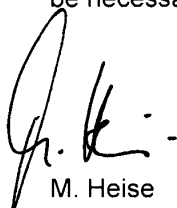
Datum / Date

EP103926-EH206mli

February 26, 2020

European Patent Application No. 14 791 882.5
Applicant: WEBROOT INC.

We herewith request to extend the term for replying to the outstanding communication by two months, as further correspondence with the Applicant will be necessary.


M. Heise

MÜNCHEN

Patentanwälte

European Patent Attorneys

Thomas Schuster
Dr. Klara Goldbach
Martin Aufenanger, LL.M., MM ¹
Dr. Heike Vogelsang-Wenke
Reinhard Knauer
Dietmar Kuhl
Dr. Franz-Josef Zimmer
Bettina K. Reichelt
Dr. Anton K. Pfau
Dr. Udo Weigelt, LL.M.
Rainer Bertram
Jens C. Koch, M.S. (U of PA)
Bernd Rothaemel
Thomas W. Laubenthal, LL.M.
Dr. Andreas Kayser
Dr. Jens Hammer
Dr. Thomas Eickelkamp
Dr. Peter Miltényi ²
Dr. Moritz Höffe, LL.M.
Gero Maatz-Jansen
Michael Heise
Christian Meisinger
Dr. Martin Ahr
Dr. Wolfgang Neubeck
Steven M. Zeman, Ph.D.
André Nickel
Felix Kahr
Dr. Alexander Stumvoll, LL.M.
Dr. Stefano Marchini ³
Dr. Thomas Kronberger
Yilin Jin
Dr. Georg Seisenberger
Dr. Olivia Nemethova, LL.M.
Dr. Rainer Plaggenborg
Victor Lopes Aguiar
Dr. Sabine Koch
Wolfram Thomas
Dr. Markus Grammel
Dr. Jegannath Korukottu ⁴

Rechtsanwälte

Attorneys-at-Law

Dr. Ulrich Blumenröder, LL.M.
Prof. Dr. Maximilian Kinkeldey, LL.M. ⁵
Dr. Karsten Brandt
Anja Franke, LL.M.
Ute Stephani
Dr. Bernd Allekotte, LL.M. ⁶
Dr. Elvira Bertram, LL.M.
Babett Ertle
Christine Neuhierl
Sabine Brandstätter
Cornelia Schmitt
Petra Lübke
Dr. Holger Gauss
Dr. Nicolás Schmitz
Marina Schlumberger
Kirsten Hammerstingl
Sebastian Clotten, LL.M.
Jennifer Rosenhäger, LL.M.
Mark Peters, LL.M.
Dr. Nicola Busch
Julia Blittner, LL.M.
Sebastian Ochs
Philipp Strommer
Jan Rether
Karin Lochner
Swetlana Frese

BERLIN

Patentanwälte

European Patent Attorneys

Dr. Patrick P. Erk, M.S. (MIT)
Tino Rumpold

KÖLN

Patentanwälte

European Patent Attorneys

Dr. Martin Drophmann
Dr. Martin Bierbaum

PARIS ⁷

Conseil en Propriété Industrielle

European Patent Attorney

Dr. Wolfgang Neubeck

OF COUNSEL

Patentanwälte

European Patent Attorneys

Gottfried Klitzsch

Rechtsanwälte

Attorneys-at-Law

Dr. Helmut Eichmann
Gerhard Barth

Grünecker Patent- und Rechtsanwälte PartG mbB

Leopoldstr. 4 Tel. +49 (0) 89 21 23 50
80802 München Fax +49 (0) 89 22 02 87
Germany Mail info@grunecker.de

Amtsgericht: München
Partnerschaftsregister:
PR 1397

Deutsche Bank München
SWIFT / BIC-code: DEUT DE MM
IBAN: DE 47 7007 0010 0175 173400

¹ auch/also: Mediator ² auch/also: Agente de la Propiedad Industrial (España) ³ auch/also: Consulente in Brevetti (Italia)

⁴ European Patent Attorney and UK Chartered Patent Attorney ⁵ Professor an der Fachhochschule für angewandtes Management

⁶ auch/also: Attorney-at-Law, New York ⁷ in Kooperation/in cooperation

Datum
Date 17.10.2019
Date

Blatt
Sheet 1
Feuille

Anmelde-Nr:
Application No: 14 791 882.5
Demande n°:

The examination is being carried out on the **following application documents**

Description, Pages

4-34 as published

1, 2, 2a, 2b, 3 received on 09-06-2017 with letter of 09-06-2017

Claims, Numbers

1-15 received on 26-03-2019 with letter of 26-03-2019

Drawings, Sheets

1/15-15/15 as published

Reference is made to the following documents

- D1 WO 2012/110501 A1 (PREVX LTD [GB]; MORRIS MELVYN [GB]; JAROCH JOSEPH [US]) 23 August 2012 (2012-08-23)
- D2 US 2008/244694 A1 (NEYSTADT JOHN [IL] ET AL) 2 October 2008 (2008-10-02)
- D3 WO 2006/094228 A2 (MARKMONITOR INC [US]; SHULL MARK [US]; BOHLMAN WILLIAM [US]; SHRAIM IH) 8 September 2006 (2006-09-08)

1 Amended claim 1 not new over D1

- 1.1 With the letter dated 26.03.2019 the applicant has submitted an amended claim 1 now additionally specifying:
- caching the one or more events and dropping events which are duplicates of recent events.*
- 1.2 The applicant identifies this feature as the difference over D1 and argues that a technical effect of caching of events combined with the dropping of duplicate events could ensure that redundant events are not continually reported since events tend to be very raw and not individually useful.
- 1.3 D1 recognizes the problem that the amount of data is vast and that it is impractical to store all data (page 31, first paragraph).
-

EPO Form 2906 01.91TRI

As a solution D1 discloses on page 31 second paragraph a database (62) of objects that have previously been seen. When data is received, the database (62) is queried. If it is determined that the object is stored in the database (62) and thus has already been previously seen, only a count associated with that data is increased without further processing the data. D1 explicitly refers to "events" as incoming data:

"... the web server 61 just increases the count associated with that checksum in its database of the number of times that data has been seen to assist in determining the popularity of a piece of software or the frequency of the occurrence of a specific event" (D1, page 31 lines 6-16).

- 1.4 Storing previously seen events in a database corresponds to "*caching the one or more events*" and only processing incoming event data which has no entry in the database corresponds to "*dropping events which are duplicates of recent events*".
- 1.5 This feature is therefore also disclosed in D1 and claim 1 still lacks novelty over D1 (Art. 54 EPC).



European Patent Office
80293 MUNICH
GERMANY
Tel: +49 89 2399 0
Fax: +49 89 2399 4465



Grünecker Patent- und Rechtsanwälte
PartG mbB
Leopoldstraße 4
80802 München
ALLEMAGNE

Formalities Officer
Name: Gottar, Chantal
Tel: +49 89 2399 - 3203
or call
+31 (0)70 340 45 00

Substantive Examiner
Name: Dingel, Janis
Tel: +49 89 2399 - 5473

Application No. 14 791 882.5 - 1218	Ref. EP103926EHjet	Date 17.10.2019
Applicant Webroot Inc.		

Communication pursuant to Article 94(3) EPC

The examination of the above-identified application has revealed that it does not meet the requirements of the European Patent Convention for the reasons enclosed herewith. If the deficiencies indicated are not rectified the application may be refused pursuant to Article 97(2) EPC.

You are invited to file your observations and insofar as the deficiencies are such as to be rectifiable, to correct the indicated deficiencies within a period

of 4 months

from the notification of this communication, this period being computed in accordance with Rules 126(2) and 131(2) and (4) EPC. One set of amendments to the description, claims and drawings is to be filed within the said period on separate sheets (R. 50(1) EPC).

If filing amendments, you must identify them and indicate the basis for them in the application as filed. Failure to meet either requirement may lead to a communication from the Examining Division requesting that you correct this deficiency (R. 137(4) EPC).

Failure to comply with this invitation in due time will result in the application being deemed to be withdrawn (Art. 94(4) EPC).

Registered letter

EPO Form 2001 11.16TRI



Dingel, Janis
Primary Examiner
For the Examining Division

Enclosure(s): 2 page/s reasons (Form 2906)

EP Application No.: 14 791 882.5
Applicant: WEBROOT INC.
Our Ref.: EP103926EH206
Date: March 26, 2019

CLAIMS (marked-up copy)

1. A method comprising:

gathering one or more events (504A-520A; 1208) defining an action of a first object (1232) acting on a target (1236);

caching the one or more events and dropping events which are duplicates of recent events;

consolidating and normalizing the one or more events;

generating a contextual state (524; 1216) for at least one of the one or more consolidated and normalized events by correlating (912) 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 (1244) on which the first object is executed and a user (1248) associated with the first object;

obtaining a global perspective for the at least one event by obtaining information (228; 528-536) associated with one or more of the first object and the originating object, the information including at least one of age (1260), popularity (1264), a determination (1268) 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 (1272);

assembling (624) an event line (244A-B) 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 (628) the assembled event line.

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

wherein the event line is transmitted to an end recipient (220).

3. The method of claim 1 or 2, further comprising:

obtaining (1112) 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 any one of claims 1 to 3, 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; and/or

further comprising:

determining (1008) 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 (1020) 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 (1016) a global perspective for the at least one event from a community database.

5. The method of claim 4, further comprising:

determining (1012) 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 (1016) a global perspective for the at least one event from a community database; and/or

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 (1260) of the first object; and a number of concurrent connections associated with the first object.

6. A computer readable storage medium comprising processor executable instructions operable to perform the method of any one of claims 1 to 5.
7. A system for providing forensic visibility into a system, comprising:

a device (204) including:

a communication interface (332);

a processor (316);

data storage (320); and

a sensor agent (208) stored on the data storage that is executable by the processor, wherein the sensor agent is operable to:

gather one or more events (504A-520A; 1208) defining an action of a first object (1232) acting on a target (1236);

cache the one or more events and drop events which are duplicates of recent events;

consolidate and normalize the one or more events;

generate a contextual state (524; 1216) for at least one of the one or more consolidated and normalized events by correlating (912) 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 (1244) on which the first object is executed and a user (1248) associated with the first object;

assemble (624) an event line (244A-B) 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 (628) the assembled event line utilizing the communication interface.

8. The system of claim 7, further comprising a global perspective information server (216) including:

a processor (464);

a communication interface (468);

data storage (488); and

a global perspective module (476), 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 (228; 528-536) associated with one or more of the first object and the originating object, the information including at least one of age (1260), popularity (1264), a determination (1268) 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 (1272);

assemble (624) 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 (628) the assembled second event line utilizing the communication interface to an end recipient (220).

9. The system of claim 7 or 8, 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 (1260) of the first object; and a number of concurrent connections associated with the first object; and/or

further comprising a bridge (222) including:

a processor (382);

a communication interface (386); and

a cached event store (394), 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 (228; 528-536) associated with one or more of the first object and the originating object, the information including at least one of age (1260), popularity (1264), a determination (1268) 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 (1272);

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.

10. The system of claim 7, wherein the sensor agent is further operable to:

obtain a global perspective for the at least one event by obtaining information (228) associated with one or more of the first object and the originating object, the information including at least one of age (1260), popularity (1264), a determination (1268) 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 (1272);

11. The system of claim 10, wherein the at least one of the one or more events is executed by the processor.
12. The system of claim 10 or 11, further comprising:
a global perspective information server (216); and
an end recipient device (220), 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.
13. The system of any one of claims 10 to 12, wherein the at least one event includes information uniquely identifying the object performing the action, information uniquely identifying the action being performed, and information uniquely identifying the target upon which the act is being performed.
14. The system of any one of claims 10 to 13, wherein the sensor agent is one or more of:
further operable to:
determine (1008) 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 (1020) 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 (1016) a global perspective for the at least one event from a community database;
or
further operable to:
determine (1012) 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 (1016) a global perspective for the at least one event from a community database.

15. 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 (1260) of the first object; and a number of concurrent connections associated with the first object.

EP Application No.: 14 791 882.5
Applicant: WEBROOT INC.
Our Ref.: EP103926EH206
Date: March 26, 2019

CLAIMS

1. A method comprising:

gathering one or more events (504A-520A; 1208) defining an action of a first object (1232) acting on a target (1236);

caching the one or more events and dropping events which are duplicates of recent events;

consolidating and normalizing the one or more events;

generating a contextual state (524; 1216) for at least one of the one or more consolidated and normalized events by correlating (912) 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 (1244) on which the first object is executed and a user (1248) associated with the first object;

obtaining a global perspective for the at least one event by obtaining information (228; 528-536) associated with one or more of the first object and the originating object, the information including at least one of age (1260), popularity (1264), a determination (1268) 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 (1272);

assembling (624) an event line (244A-B) 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 (628) the assembled event line.
2. The method of claim 1, wherein the information associated with the one or more of the first object and the originating object is obtained from a community database; and
wherein the event line is transmitted to an end recipient (220).
3. The method of claim 1 or 2, further comprising:

obtaining (1112) 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 any one of claims 1 to 3, 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; and/or

further comprising:

determining (1008) 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 (1020) 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 (1016) a global perspective for the at least one event from a community database.

5. The method of claim 4, further comprising:

determining (1012) 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 (1016) a global perspective for the at least one event from a community database; and/or

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 (1260) of the first object; and a number of concurrent connections associated with the first object.

6. A computer readable storage medium comprising processor executable instructions operable to perform the method of any one of claims 1 to 5.
7. A system for providing forensic visibility into a system, comprising:

a device (204) including:

a communication interface (332);

a processor (316);

data storage (320); and

a sensor agent (208) stored on the data storage that is executable by the processor, wherein the sensor agent is operable to:

gather one or more events (504A-520A; 1208) defining an action of a first object (1232) acting on a target (1236);

cache the one or more events and drop events which are duplicates of recent events;

consolidate and normalize the one or more events;

generate a contextual state (524; 1216) for at least one of the one or more consolidated and normalized events by correlating (912) 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 (1244) on which the first object is executed and a user (1248) associated with the first object;

assemble (624) an event line (244A-B) 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 (628) the assembled event line utilizing the communication interface.

8. The system of claim 7, further comprising a global perspective information server (216) including:

a processor (464);

a communication interface (468);

data storage (488); and

a global perspective module (476), 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 (228; 528-536) associated with one or more of the first object and the originating object, the information including at least one of age (1260), popularity (1264), a determination (1268) 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 (1272);

assemble (624) 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 (628) the assembled second event line utilizing the communication interface to an end recipient (220).

9. The system of claim 7 or 8, 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 (1260) of the first object; and a number of concurrent connections associated with the first object; and/or

further comprising a bridge (222) including:

a processor (382);

a communication interface (386); and

a cached event store (394), 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 (228; 528-536) associated with one or more of the first object and the originating object, the information including at least one of age (1260), popularity (1264), a determination (1268) 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 (1272);

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.

10. The system of claim 7, wherein the sensor agent is further operable to:

obtain a global perspective for the at least one event by obtaining information (228) associated with one or more of the first object and the originating object, the information including at least one of age (1260), popularity (1264), a determination (1268) 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 (1272);

11. The system of claim 10, wherein the at least one of the one or more events is executed by the processor.
12. The system of claim 10 or 11, further comprising:
a global perspective information server (216); and
an end recipient device (220), 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.
13. The system of any one of claims 10 to 12, wherein the at least one event includes information uniquely identifying the object performing the action, information uniquely identifying the action being performed, and information uniquely identifying the target upon which the act is being performed.
14. The system of any one of claims 10 to 13, wherein the sensor agent is one or more of:
further operable to:
determine (1008) 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 (1020) 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 (1016) a global perspective for the at least one event from a community database;
or
further operable to:
determine (1012) 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 (1016) a global perspective for the at least one event from a community database.

15. 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 (1260) of the first object; and a number of concurrent connections associated with the first object.

European Patent Office

Bob-van-Benthem-Platz 1
80469 München

EPO - Munich
102

26. März 2019

Ihr Zeichen / Your Ref.

Unser Zeichen / Our Ref.

Datum / Date

EP103926EH206amr

March 26, 2019

European Patent Application No. 14 791 882.5
Applicant: WEBROOT INC.

In response to the Official Communication pursuant to Article 94(3) EPC dated
November 16, 2018:

Submitted herewith are:

- new claims 1 to 15 to replace all claims presently on file.

Also enclosed is a marked-up version of the new claim set, highlighting all claim amendments.

The claims have been amended in order to overcome all objections raised in the above-mentioned Official Communication.

I. Amendments

New independent claim 1 is based on previously submitted claim 1 and further defines dropping events which are duplicates of recent events. This amendment can be derived from the application as originally filed, including page 3, line 24, page 15, lines 25 to 27, page 25, line 6 and page 27, lines 6 to 10.

New dependent claims 2 to 5 are identical to previously submitted claims 2 to 5, respectively.

Grünecker Patent- und Rechtsanwälte PartG mbB

Leopoldstr. 4	Tel. +49 (0) 89 21 23 50	Amtsgericht: München	Deutsche Bank München
80802 München	Fax +49 (0) 89 22 02 87	Partnerschaftsregister:	SWIFT / BIC-code: DEUT DE MM
Germany	Mail info@grunecker.de	PR 1397	IBAN: DE 47 7007 0010 0175 173400

¹ auch/also: Mediator ² auch/also: Agente de la Propiedad Industrial (España) ³ auch/also: Consulente in Brevetti (Italia)

⁴ auch/also: UK Chartered Patent Attorney ⁵ Professor an der Fachhochschule für angewandtes Management

⁶ auch/also: Attorney-at-Law, New York ⁷ in Kooperation/in cooperation

MÜNCHEN

Patentanwälte
European Patent Attorneys
Hans Hilgers
Thomas Schuster
Dr. Klara Goldbach
Martin Aufenanger, LL.M., MM ¹
Dr. Heike Vogelsang-Wenke
Reinhard Knauer
Dietmar Kuhl
Dr. Franz-Josef Zimmer
Bettina K. Reichelt
Dr. Anton K. Pfau
Dr. Udo Weigelt, LL.M.
Rainer Bertram
Jens C. Koch, M.S. (U of PA)
Bernd Rothaemel
Thomas W. Laubenthal, LL.M.
Dr. Andreas Kayser
Dr. Jens Hammer
Dr. Thomas Eickelkamp
Dr. Peter Miltényi ²
Dr. Moritz Höffe, LL.M.
Gero Maatz-Jansen
Michael Heise
Christian Meisinger
Dr. Martin Ahr
Dr. Wolfgang Neubeck
Steven M. Zeman, Ph.D.
André Nickel
Felix Kahr
Dr. Alexander Sturmvoll, LL.M.
Dr. Stefano Marchini ³
Dr. Thomas Kronberger
Yilin Jin
Dr. Georg Seisenberger
Dr. Olivia Nemethova, LL.M.
Dr. Rainer Plaggenborg
Victor Lopes Aguiar
Dr. Sabine Koch
Wolfram Thomas
Dr. Markus Grammel
Dr. Jegannath Korukottu ⁴

Rechtsanwälte

Attorneys-at-Law
Dr. Ulrich Blumenröder, LL.M.
Prof. Dr. Maximilian Kinkeldey, LL.M. ⁵
Dr. Karsten Brandt
Anja Franke, LL.M.
Ute Stephan
Dr. Bernd Allekotte, LL.M. ⁶
Dr. Elvira Bertram, LL.M.
Babett Ertle
Christine Neuhierl
Sabine Brandstätter
Cornelia Schmitt
Petra Lübke
Dr. Holger Gauss
Dr. Nicolás Schmitz
Marina Schlumberger
Kirsten Hammerstingl
Sebastian Clotten, LL.M.
Jennifer Rosenhäger, LL.M.
Mark Peters, LL.M.
Dr. Nicola Busch
Julia Bittner, LL.M.
Sebastian Ochs
Philipp Strommer
Jan Rether
Karin Lochner
Swetlana Frese

BERLIN

Patentanwälte
European Patent Attorneys
Dr. Patrick P. Erk, M.S. (MIT)
Dr. Svenja Sethmann
Tino Rumpold

KÖLN

Patentanwälte
European Patent Attorneys
Dr. Martin Dropmann

PARIS ⁷

Conseil en Propriété Industrielle
European Patent Attorney
Dr. Wolfgang Neubeck

OF COUNSEL

Patentanwälte
European Patent Attorneys
Gottfried Klitzsch

Rechtsanwälte
Attorneys-at-Law
Dr. Helmut Eichmann
Gerhard Barth

New claim 6 corresponds to previously submitted claim 6.

New independent claim 7 is based on previously submitted claim 7 and has been amended in the same manner as corresponding claim 1.

New dependent claims 8 to 15 are identical to previously submitted claims 8 to 15, respectively.

Accordingly, the claims do not introduce subject matter extending beyond the content of the application as originally filed and fulfill the requirements of Article 123(2) EPC.

II. Patentability

The Examining Division's arguments and analysis concerning the cited prior art documents are highly appreciated and have been carefully considered and taken into account. However, in regard to the new claims, the Examining Division is kindly requested to consider the following arguments, which lead to the conclusion that the claimed subject matter is novel and involves an inventive step over the available prior art.

In particular, it is respectfully submitted that although D1 seems to suggest that the local database stores a signature of an object and/or its related event, D1 does not disclose dropping duplicate events. Moreover, it is respectfully pointed out that D1 seems to store a signature of an event in the local database 11 but not an event itself.

In view of the aforementioned distinguishing features, the claimed subject matter is considered to be novel within the meaning of Article 54 EPC.

Similarly, it is respectfully pointed out that these distinguishing features are also not disclosed or suggested by the remaining cited documents D2 and D3.

In addition, it is respectfully submitted that caching the events and dropping duplicate events allows an intelligent processing to be carried out. Events usually tend to be very raw and generally not individually useful (tens of millions of events could 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. The caching of events combined with the dropping of duplicate events could ensure that redundant events are not continually reported (many applications perform thousands of the

same events and transmitting these events into an external log source would create a significant amount of unnecessary noise and potential performance degradation).

Since neither D1 nor the remaining prior art disclose or suggest the aforementioned distinguishing features, the claimed subject matter does not arise from the available prior art in an obvious manner, but involves an inventive step within the meaning of Article 56 EPC.

III. Summary

As the new claims submitted herewith are considered to overcome all objections raised in the above mentioned Official Communication, the Examining Division is kindly requested to propose grant.

Should the Examining Division have further objections against the present application, it is kindly and respectfully requested that the proceedings be continued in writing by issuing a further examination report. As a measure of precaution only, the request for oral proceedings is maintained.



M. Heise

Encl.
Claims 1 to 15 (clean and marked-up copies)

Datum
Date 16.11.2018
Date

Blatt
Sheet 1
Feuille

Anmelde-Nr:
Application No: 14 791 882.5
Demande n°:

The examination is being carried out on the **following application documents**

Description, Pages

4-34 as published

1, 2, 2a, 2b, 3 received on 09-06-2017 with letter of 09-06-2017

Claims, Numbers

1-15 received on 18-04-2018 with letter of 18-04-2018

Drawings, Sheets

1/15-15/15 as published

Reference is made to the following document:

D1 WO 2012/110501 A1 (PREVX LTD [GB]; MORRIS MELVYN [GB];
JAROCH JOSEPH [US]) 23 August 2012 (2012-08-23)

1 Amended claim 1 still not novel

1.1 The present application does not meet the requirements of Article 52(1) EPC because the subject-matter of amended claim 1 is still not new within the meaning of Article 54(1) and (2) EPC.

1.2 The applicant has submitted an amended claim 1 with the letter dated 18.04.2018. The applicant has amended claim 1 to include the features

- *caching the one or more events*

- *consolidating and normalizing the one or more events*

taken from the description.

1.3 The Examiner has carefully considered the arguments submitted by the applicant in the letter and is, however, still of the opinion that claim 1 lacks novelty over D1 for the following reasons:

1.4 Caching the one or more events

1.4.1 According to Wikipedia ([https://en.wikipedia.org/wiki/Cache_\(computing\)](https://en.wikipedia.org/wiki/Cache_(computing))): "*In computing, a **cache** [...] is a hardware or software component that stores data so that future requests for that data can be served faster*".

1.4.2 That is, "*caching the one or more events*" does not imply dropping of events which are duplicates of recent events as submitted by the applicant on page 2, last paragraph of the letter.

1.4.3 Fig. 3 of D1 discloses a local database 11 within the remote computer 2. With reference to Figure 2 it is disclosed in D1 that event data is stored in the local database: "*...the agent program can search a local database stored at the remote computer 2 to search for a signature or key representing that particular process, its related objects and/or the event*".

Note that an "object" in the sense of D1 may also be an event: "*An object in this sense may be [...] any other event whether executed, emulated, simulated or interpreted*" (D1, p.16, ll.21-23).

1.4.4 The method in D1 first consults the local database 11 to determine whether an object is classified malicious before sending details of an object to a global database 74: "*The agent program 10 optionally communicates with a local database 11 which holds a local copy of signatures relating to the objects found on the remote computer 2*" (D1, p.24, ll.24-26). This allows to faster classify objects/events in case an event is stored in the local database and thus represents a form of caching according to the definition given above.

1.4.5 The storing of objects (i.e. events) in the local database in D1 therefore corresponds to "*caching the one or more events*" according to claim 1.

1.5 Consolidating and normalizing the one or more events

1.5.1 With regards to the new features "*consolidating and normalizing the one or more events*" it is noted that "consolidating" and "normalizing" have no well defined meaning within the technical context of the invention, and thus must be interpreted broadly.

1.5.2 D1 discloses organising an event in a data structure with three principal components (Actor, Event Type, Victim) (D1, p.21, l.31 - p.22, l.15). Processing events to conform with such a well defined data structure can be regarded to fall under the broad scope of "*consolidating and normalizing the one or more events*".

- 1.5.3 According to the description of the present application normalization is the process of organising items such as process objects, filenames etc. in a standard format which is more easily consumed by automated parsers. The data structure shown on page 22 of D1 also represents a standard format in that sense, and can therefore also be regarded as "normalization".
- 1.5.4 Furthermore, D1 discloses "Event Checksums" which can also be regarded as normalization and consolidation. Even if arguing that a checksum does not correspond to a normalization, in D1 checksums are used to determine whether an event with identical checksum has been recorded previously. Matching checksums of data for this purpose implies that data is normalized (standardized) before the checksum is calculated because otherwise two identical events could not be matched by their checksum.
- 1.6 Amended claim 1 is therefore not new over D1 (Art. 54 EPC). With regards to the objections raised in the previous and present communications, a summons to Oral Proceedings under Art. 116(1) EPC (if still requested) with the likely outcome of a refusal of the application under Art. 97(2) EPC is to be expected, if the above-mentioned major deficiencies (lack of novelty under Art. 54) of the present application are not remedied at the next stage of the procedure.



European Patent Office
80293 MUNICH
GERMANY
Tel: +49 89 2399 0
Fax: +49 89 2399 4465



Grünecker Patent- und Rechtsanwälte
PartG mbB
Leopoldstraße 4
80802 München
ALLEMAGNE

Formalities Officer
Name: Gottar, Chantal
Tel: +49 89 2399 - 3203
or call
+31 (0)70 340 45 00

Substantive Examiner
Name: Dingel, Janis
Tel: +49 89 2399 - 5473

Application No. 14 791 882.5 - 1218	Ref. EP103926EHjet	Date 16.11.2018
Applicant Webroot Inc.		

Communication pursuant to Article 94(3) EPC

The examination of the above-identified application has revealed that it does not meet the requirements of the European Patent Convention for the reasons enclosed herewith. If the deficiencies indicated are not rectified the application may be refused pursuant to Article 97(2) EPC.

You are invited to file your observations and insofar as the deficiencies are such as to be rectifiable, to correct the indicated deficiencies within a period

of 4 months

from the notification of this communication, this period being computed in accordance with Rules 126(2) and 131(2) and (4) EPC. One set of amendments to the description, claims and drawings is to be filed within the said period on separate sheets (R. 50(1) EPC).

If filing amendments, you must identify them and indicate the basis for them in the application as filed. Failure to meet either requirement may lead to a communication from the Examining Division requesting that you correct this deficiency (R. 137(4) EPC).

Failure to comply with this invitation in due time will result in the application being deemed to be withdrawn (Art. 94(4) EPC).

Registered letter

EPO Form 2001 11.16TRI



Dingel, Janis
Primary Examiner
For the Examining Division

Enclosure(s): 3 page/s reasons (Form 2906)

EP Application No.: 14 791 882.5
Applicant: WEBROOT INC.
Our Ref.: EP103926EH206
Date: April 18, 2018

5

NEW CLAIMS (marked-up copy highlighting all amendments)

1. A method comprising:

10

gathering one or more events (504A-520A; 1208) defining an action of a first object (1232) acting on a target (1236);

caching the one or more events;

consolidating and normalizing the one or more events;

15

generating a contextual state (524; 1216) for at least one of the one or more consolidated and normalized events by correlating (912) 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 (1244) on which the first object is executed and a user (1248) associated with the first object;

20

obtaining a global perspective for the at least one event by obtaining information (228; 528-536) associated with one or more of the first object and the originating object, the information including at least one of age (1260), popularity (1264), a determination (1268) 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 (1272);

25

assembling (624) an event line (244A-B) 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 (628) the assembled event line.

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

30

wherein the event line is transmitted to an end recipient (220).

3. The method of claim 1 or 2, further comprising:

obtaining (1112) 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 any one of claims 1 to 3, 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; and/or
- 5 further comprising:
- determining (1008) 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 (1020) a global perspective for the at least one event based on the
- 10 cached global perspective; and
- when the global perspective for the at least one event has not been cached, obtaining (1016) a global perspective for the at least one event from a community database.
5. The method of claim 4, further comprising:
- 15 determining (1012) 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 (1016) a global perspective for the at least one event from a community database; and/or
- further comprising:
- 20 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 (1260) of
- 25 the first object; and a number of concurrent connections associated with the first object.
6. A computer readable storage medium comprising processor executable instructions operable to perform the method of any one of claims 1 to 5.
7. A system for providing forensic visibility into a system, comprising:
- a device (204) including:
- 30 a communication interface (332);
- a processor (316);

data storage (320); and

a sensor agent (208) stored on the data storage that is executable by the processor, wherein the sensor agent is operable to:

gather one or more events (504A-520A; 1208) defining an action of a first object (1232) acting on a target (1236);

cache the one or more events;

consolidate and normalize the one or more events;

generate a contextual state (524; 1216) for at least one of the one or more consolidated and normalized events by correlating (912) 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 (1244) on which the first object is executed and a user (1248) associated with the first object;

assemble (624) an event line (244A-B) 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 (628) the assembled event line utilizing the communication interface.

8. The system of claim 7, further comprising a global perspective information server (216) including:

a processor (464);

a communication interface (468);

data storage (488); and

a global perspective module (476), 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 (228; 528-536) associated with one or more of the first object and the originating object, the information including at least one of age (1260), popularity (1264), a determination (1268) 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 (1272);

assemble (624) 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

5 transmit (628) the assembled second event line utilizing the communication interface to an end recipient (220).

9. The system of claim 7 or 8, 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
10 object; at least one characteristic of an outbound connection associated with the first object; a dropped executable file; an age (1260) of the first object; and a number of concurrent connections associated with the first object; and/or

further comprising a bridge (222) including:

a processor (382);

15 a communication interface (386); and

a cached event store (394), 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;

20 obtain a first global perspective for the at least one event by obtaining information (228; 528-536) associated with one or more of the first object and the originating object, the information including at least one of age (1260), popularity (1264), a determination (1268) as to whether the first object is malware, a determination as to whether the originating object is malware; and Internet Protocol, IP, Address or
25 Uniform Resource Locator, URL, information (1272);

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.

10. The system of claim 7, wherein the sensor agent is further operable to:

30 obtain a global perspective for the at least one event by obtaining information (228) associated with one or more of the first object and the originating object, the information including at least one of age (1260), popularity (1264), a

determination (1268) 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 (1272);

11. The system of claim 10, wherein the at least one of the one or more events is executed by the processor.
12. The system of claim 10 or 11, further comprising:
 - a global perspective information server (216); and
 - an end recipient device (220), 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.
13. The system of any one of claims 10 to 12, wherein the at least one event includes information uniquely identifying the object performing the action, information uniquely identifying the action being performed, and information uniquely identifying the target upon which the act is being performed.
14. The system of any one of claims 10 to 13, wherein the sensor agent is one or more of:
 - determine (1008) 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 (1020) 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 (1016) a global perspective for the at least one event from a community database; or
- further operable to:
 - determine (1012) 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 (1016) a global perspective for the at least one event from a community database; or
- ~~further operable to:~~
 - ~~cache the one or more events, and~~

~~asynchronously consolidate and normalize (816) the one or more events.~~

15. 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 (1260) of the first object; and a number of concurrent connections associated with the first object.

10

EP Application No.: 14 791 882.5
Applicant: WEBROOT INC.
Our R f.: EP103926EH206
Date: April 18, 2018

5

CLAIMS

1. A method comprising:

10 gathering one or more events (504A-520A; 1208) defining an action of a first object (1232) acting on a target (1236);

 caching the one or more events;

 consolidating and normalizing the one or more events;

15 generating a contextual state (524; 1216) for at least one of the one or more consolidated and normalized events by correlating (912) 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 (1244) on which the first object is executed and a user (1248) associated with the first object;

20 obtaining a global perspective for the at least one event by obtaining information (228; 528-536) associated with one or more of the first object and the originating object, the information including at least one of age (1260), popularity (1264), a determination (1268) 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 (1272);

25 assembling (624) an event line (244A-B) 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 (628) the assembled event line.
2. The method of claim 1, wherein the information associated with the one or more of the first object and the originating object is obtained from a community database; and
- 30 wherein the event line is transmitted to an end recipient (220).
3. The method of claim 1 or 2, further comprising:

obtaining (1112) 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 any one of claims 1 to 3, 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; and/or
- 5 further comprising:
- determining (1008) 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 (1020) a global perspective for the at least one event based on the
- 10 cached global perspective; and
- when the global perspective for the at least one event has not been cached, obtaining (1016) a global perspective for the at least one event from a community database.
5. The method of claim 4, further comprising:
- 15 determining (1012) 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 (1016) a global perspective for the at least one event from a community database; and/or
- further comprising:
- 20 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 (1260) of
- 25 the first object; and a number of concurrent connections associated with the first object.
6. A computer readable storage medium comprising processor executable instructions operable to perform the method of any one of claims 1 to 5.
7. A system for providing forensic visibility into a system, comprising:
- a device (204) including:
- 30 a communication interface (332);
- a processor (316);

data storage (320); and

a sensor agent (208) stored on the data storage that is executable by the processor, wherein the sensor agent is operable to:

- 5 gather one or more events (504A-520A; 1208) defining an action of a first object (1232) acting on a target (1236);
- cache the one or more events;
- consolidate and normalize the one or more events;
- 10 generate a contextual state (524; 1216) for at least one of the one or more consolidated and normalized events by correlating (912) 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 (1244) on which the first object is executed and a user (1248) associated with the first object;
- 15 assemble (624) an event line (244A-B) 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 (628) the assembled event line utilizing the communication interface.

8. The system of claim 7, further comprising a global perspective information server (216) including:

- 20 a processor (464);
- a communication interface (468);
- data storage (488); and
- a global perspective module (476), wherein the global perspective module is operable to:
 - 25 receive the event line from the device;
 - obtain a global perspective for the at least one event by obtaining information (228; 528-536) associated with one or more of the first object and the originating object, the information including at least one of age (1260), popularity (1264), a determination (1268) as to whether the first object is malware, a determination as to whether the originating object is malware; and Internet Protocol, IP, Address or
 - 30 Uniform Resource Locator, URL, information (1272);

assemble (624) 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

5 transmit (628) the assembled second event line utilizing the communication interface to an end recipient (220).

9. The system of claim 7 or 8, 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 (1260) of the first object; and a number of concurrent connections associated with the first object; and/or

further comprising a bridge (222) including:

a processor (382);

15 a communication interface (386); and

a cached event store (394), 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;

20 obtain a first global perspective for the at least one event by obtaining information (228; 528-536) associated with one or more of the first object and the originating object, the information including at least one of age (1260), popularity (1264), a determination (1268) 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 (1272);

25 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.

10. The system of claim 7, wherein the sensor agent is further operable to:

30 obtain a global perspective for the at least one event by obtaining information (228) associated with one or more of the first object and the originating object, the information including at least one of age (1260), popularity (1264), a

determination (1268) 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 (1272);

11. The system of claim 10, wherein the at least one of the one or more events is executed by the processor.
12. The system of claim 10 or 11, further comprising:
a global perspective information server (216); and
an end recipient device (220), 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.
13. The system of any one of claims 10 to 12, wherein the at least one event includes information uniquely identifying the object performing the action, information uniquely identifying the action being performed, and information uniquely identifying the target upon which the act is being performed.
14. The system of any one of claims 10 to 13, wherein the sensor agent is one or more of:
further operable to:
determine (1008) 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 (1020) 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 (1016) a global perspective for the at least one event from a community database; or
further operable to:
determine (1012) 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 (1016) a global perspective for the at least one event from a community database.
15. 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 (1260) of the first object; and a number of concurrent connections associated with the first object.

5

Grünecker PartG mbB Leopoldstr. 4 80802 München Germany

European Patent Office

Bob-van-Bentham-Platz 1
80469 München

Ihr Zeichen / Your Ref.

Unser Zeichen / Our Ref.

EPO - Munich
101

18. April 2018

Datum / Date

EP103926EH206amr

April 18, 2018

European Patent Application No. 14 791 882.5

Applicant: WEBROOT INC.

In response to the Official Communication dated December 8, 2017:

Herewith submitted are:

- new claims 1 to 15 to replace all claims on file.

Also enclosed is a marked-up copy of the new claim set highlighting all claim amendments.

The independent claims have been amended in order to overcome the outstanding objection raised in the above-mentioned Official Communication.

As apparent from the marked-up copy of the new claim set, the independent claims have been amended by additionally defining the features of caching the one or more events, and consolidating and normalizing the one or more events. This amendment is derivable from the application as originally filed, including description page 3, lines 24 and 25, page 11, line 2, page 14, lines 30 and 31, page 15, lines 24 to 27, page 16, lines 20 and 21, page 25, lines 6 and 7 and page 27, lines 18 to 27.

MÜNCHEN

Patentanwälte
European Patent Attorneys
Hans Hilgers
Thomas Schuster
Dr. Klara Goldbach
Martin Aufenanger, LL.M., MM.¹
Gottfried Klitzsch
Dr. Heike Vogelsang-Wanke
Reinhard Knauer
Dietmar Kuhl
Dr. Franz-Josef Zimmer
Bettina K. Reichelt
Dr. Anton K. Plau
Dr. Udo Weigelt, LL.M.
Rainer Bertram
Jens C. Koch, M.S. (U of PA)
Bernd Rothaemel
Thomas W. Laubenthal, LL.M.
Dr. Andreas Kayser
Dr. Jens Hammer
Dr. Thomas Eickelkamp
Dr. Peter Miltényi²
Dr. Moritz Höffe, LL.M.
Gero Maatz-Jansen
Michael Heise
Christian Meisinger
Dr. Martin Ahr
Dr. Wolfgang Neubeck
Steven M. Zeman, Ph.D.
André Nickel
Felix Kahr
Dr. Alexander Stumvoll, LL.M.
Dr. Stefano Marchini³
Dr. Thomas Kronberger
Yilin Jin
Dr. Georg Seisenberger
Dr. Olivia Nemethova, LL.M.
Dr. Rainer Plaggenborg
Victor Lopes Aguiar
Dr. Sabine Koch
Wolfram Thomas

Rechtsanwälte

Attorneys-at-Law
Dr. Helmut Eichmann
Gerhard Barth
Dr. Ulrich Blumenröder, LL.M.
Prof. Dr. Maximilian Kinkeldey, LL.M.⁴
Dr. Karsten Brandt
Anja Franke, LL.M.
Ute Stephani
Dr. Bernd Allekotte, LL.M.⁵
Dr. Elvira Bertram, LL.M.
Babett Ertle
Christine Neuhiel
Sabine Brandstätter
Cornelia Schmitt
Petra Lübke
Dr. Holger Gauss
Dr. Nicolás Schmitz
Marina Schlumberger
Kirsten Hammerstingl
Sebastian Clotten, LL.M.
Jennifer Rosenhäger, LL.M.
Mark Peters, LL.M.
Dr. Nicola Busch
Julia Bittner, LL.M.
Sebastian Ochs
Philipp Strommer
Jan Rether
Karin Lochner

BERLIN

Patentanwälte
European Patent Attorneys
Dr. Patrick P. Erk, M.S. (MIT)
Dr. Svenja Sethmann
Tino Rumpold

KÖLN

Patentanwälte
European Patent Attorneys
Dr. Martin Dropmann

PARIS⁶

Conseil en Propriété Industrielle
European Patent Attorney
Dr. Wolfgang Neubeck

Grünecker Patent- und Rechtsanwälte PartG mbB

Leopoldstr. 4 Tel. +49 (0) 89 21 23 50
80802 München Fax +49 (0) 89 22 02 87
Germany Mail info@grunecker.de

Amtsgericht: München
Partnerschaftsregister:
PR 1397

Deutsche Bank München
SWIFT / BIC-code: DEUT DE MM
IBAN: DE47 7007 0010 0175 173400

¹ auch/also: Mediator ² auch/also: Agente de la Propiedad Industrial (España) ³ auch/also: Consulente in Brevetti (Italia)
⁴ Professor an der Fachhochschule für angewandtes Management ⁵ auch/also: Attorney-at-Law, New York ⁶ in Kooperation/in cooperation

At least in view of this amendment, the claimed subject matter is considered to be novel over closest prior art document D1 and to involve an inventive step since neither D1 nor the remaining documents disclose or suggest the caching of events and data consolidation and normalization prior to obtaining the contextual state and global perspective within the context of the claimed invention.

In particular, closest prior art document D1 only suggests that metadata is collected for objects, and that the metadata includes event data that define the actions or behaviors of an object acting upon another object or some entity. However, D1 does not disclose a caching of events, nor a consolidation and normalization of the events.

On the other hand, while D2 would, if at all, suggest that security assessment endpoints perform logging of local actions, and that security assessments are shared within the system, D2 does not disclose or suggest a caching of events. Similarly, D2 does not disclose a consolidation and normalization of events.

Moreover, D3 suggests that upon detection of a communication associated with an online entity, a monitoring agent may obtain one or more trust scores associated with the online entity. The monitoring agent may first determine if the trust score for the online entity is cached in a local trust cache. If not, the monitoring agent may issue a request to a trust score server for the online entity's trust score(s) (see paragraph [0086] and Figure 5 of D3).

Thus, the trust score of D3 would, if at all, correspond to the global perspective of the claimed invention. As such, D3 would, if at all, suggest a caching of the global perspective but not a caching of the events. Moreover, D3 is silent regarding the consolidation and normalization of events.

The novel concept of caching the events allows an intelligent processing to be carried out such as for example dropping events which are duplicates of recent events. Usually, events tend to be very raw and generally not individually useful (tens of millions of events could 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. The caching of events ensures that redundant events are not continually reported (i.e. many applications perform thousands of the same events and

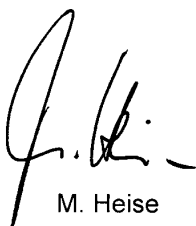
transmitting these events into an external log source would create a significant amount of unnecessary noise and potential performance degradation).

In addition, data consolidation and normalization ensure consistency. For example, data normalization could take items such as kernel filenames, user mode filenames, process objects, registry objects and other system structures and normalize them into a standard format which is more easily consumed by the subsequent processing modules. Consolidating and normalizing data at this stage allows the data to be handled more quickly while avoiding reprocessing data and potentially missing events just because they were referred to differently (\Device\HarddiskVolume1\Windows\file.exe instead of C:\Windows\file.exe for example).

In view of the above, the novel claimed invention provides an improved scheme for processing events and information related to events so as to allow an efficient forensic analysis of the events.

Consequently, the claimed subject matter is considered to be novel and to involve an inventive step.

Should the Examining Division have further objections against the present application, it is kindly and respectfully requested to continue the proceedings in writing by issuing a further examination report. As a measure of precaution, oral proceedings are requested.



M. Heise

Encl.

Claims 1 to 15 (clean and marked-up versions)

Datum
Date 08.12.2017
Date

Blatt
Sheet 1
Feuille

Anmelde-Nr:
Application No: 14 791 882.5
Demande n°:

The examination is being carried out on the **following application documents**

Description, Pages

4-34 as published

1, 2, 2a, 2b, 3 received on 09-06-2017 with letter of 09-06-2017

Claims, Numbers

1-15 received on 09-06-2017 with letter of 09-06-2017

Drawings, Sheets

1/15-15/15 as published

Reference is made to the following documents; the numbering will be adhered to in the rest of the procedure.

- D1 WO 2012/110501 A1 (PREVX LTD [GB]; MORRIS MELVYN [GB]; JAROCH JOSEPH [US]) 23 August 2012 (2012-08-23)
- D2 US 2008/244694 A1 (NEYSTADT JOHN [IL] ET AL) 2 October 2008 (2008-10-02)
- D3 WO 2006/094228 A2 (MARKMONITOR INC [US]; SHULL MARK [US]; BOHLMAN WILLIAM [US]; SHRAIM IH) 8 September 2006 (2006-09-08)

1 Arguments provided by the applicant

- 1.1 The applicant has not amended the subject-matter of the claims and has, with the letter dated 09.06.2017, submitted arguments for novelty of claim 1 with regards to the disclosure D1 cited in the European Search Report.
- 1.2 The Examiner has carefully considered the arguments submitted by the applicant and is, however, still of the opinion that claim 1 lacks novelty over D1 for the following reasons:

- 1.3 On page 4 second paragraph of the letter, the applicant argues that *"D1 does not disclose that the contextual state is generated by correlating the event to the originating object. In D1 the event data is not correlated with an originating object to generate a contextual state ... as it is not generated by correlating the event with an originating object"*.
- 1.4 In D1, metadata about an object is gathered, the metadata including "Events" and "Genesisactor". A "Genesisactor" in D1 is *".. an object that is not the direct Actor of an event but which is the ultimate parent of the event being performed. For example in the case of a software installation, this would be the key of the object that the user or system first executed and that initiated the software installation process, e.g. Setup.exe"* (D1, p.21-22). The "Genesisactor" of D1 is therefore to be equated with the "originating object" of claim 1. According to the website www.dictionary.com the term "correlating" means *"to bring or place in mutual or reciprocal relation"*. Certainly, by identifying the "Genesisactor" of an event, the event is brought in relation with the "Genesisactor". D1 therefore discloses the gathering of events, and the "correlating" of the events with an originating object ("Genesisactor") resulting in the metadata.
- 1.5 The applicant further argues that *"the identity of the remote computer and the creator of the file are separate from the metadata, and cannot correspond to a contextual state for the event included in the metadata"*, referring to page 39, lines 3 to 12 of D1.

However, the passage cited by the applicant referring to the table 105 representing *"information about the objects"* states that *"the information may include any of the data collected about an object, its metadata or its behaviour"*.

The "information about the objects" therefore includes the *"indication of the originating of the first object"* of claim 1 ("Genesisactor" in metadata in D1), the *"indication of at least one of a device on which the first object is executed"* of claim 1 (the identity of the remote computer that encountered the object in D1) and the *"user associated with the first object"* of claim 1 (the creator of the file in D1). Since the "information about the objects" in D1 also includes the events (as part of the metadata), each event can be associated with the other information included in the "information about the objects" which can therefore be regarded as a *"contextual state for at least one of the one or more events"*.

- 1.6 The applicant argues further, on page 4 paragraph 4 of the letter, that "*D1 is silent regarding obtaining a global perspective for the event*". In D1 the agent program of a remote computer, after gathering the metadata and information about an object, communicates with a (global) base computer, the base computer querying a database for deciding and communicating to the remote computer whether the object is safe (D1, Fig. 3 and p.25,l.28 - p.26,l.14).
- D1 therefore discloses "*obtaining a global perspective*". The web server searches the database based on a signature received from the remote computer. According to D1 (same passage): "*the signature can be a function of ... event data involving the object*". Therefore, D1 discloses obtaining the global perspective based on the event data which corresponds to the step of "*obtaining a global perspective for the event*" of claim 1.
- 1.7 Regarding the feature "*assembling an event line*" the Examiner is of the opinion that the term "*event line*" has no special well defined meaning and can be interpreted broadly as a data structure including information regarding the gathered events and including the additional data elements listed in claim 1. As pointed out above with reference to table 105, D1 discloses to assemble a data structure including metadata (including the event and "Genesisactor" data) and all the other data elements included in the "event line" of claim 1 (Table 105, Fig. 10, p.39).
- 1.8 The applicant argues that D1 deals with objects as the main entity for the analysis while the claimed invention deals with events as the main entity. The Examiner is of the opinion that D1 and the claimed invention both deal with the same technical problem which is the classification of objects executing on a client into malware and non-malware. The claimed invention solely focuses on the analysis of the event data while D1 performs the analysis using the event data (as shown above) but also including additional information on the objects. D1 therefore discloses the same subject-matter as the claimed invention.
- 1.9 It is not at present apparent which part of the application could serve as a basis for a new, allowable claim. Should the applicant nevertheless regard some particular matter as patentable, an independent claim should be filed taking account of Rule 43(1) EPC. The applicant should also indicate how the subject-matter of the new claim differs from the state of the art and the significance thereof.
- 1.10 With regards to the objections raised in the previous and present communications, a summons to Oral Proceedings under Art. 116(1) EPC (if still requested) with the likely outcome of a refusal of the application under

Datum
Date 08.12.2017
Date

Blatt
Sheet 4
Feuille

Anmelde-Nr:
Application No: 14 791 882.5
Demande n°:

Art. 97(2) EPC is to be expected, if the above-mentioned major deficiencies (lack of novelty under Art. 54) of the present application are not remedied at the next stage of the procedure.



European Patent Office
80293 MUNICH
GERMANY
Tel: +49 89 2399 0
Fax: +49 89 2399 4465



Grünecker Patent- und Rechtsanwälte
PartG mbB
Leopoldstraße 4
80802 München
ALLEMAGNE

Formalities Officer
Name: Gottar, Chantal
Tel: +49 89 2399 - 3203
or call
+31 (0)70 340 45 00

Substantive Examiner
Name: Dingel, Janis
Tel: +49 89 2399 - 5473

Application No. 14 791 882.5 - 1870	Ref. EP103926EHjet	Date 08.12.2017
Applicant Webroot Inc.		

Communication pursuant to Article 94(3) EPC

The examination of the above-identified application has revealed that it does not meet the requirements of the European Patent Convention for the reasons enclosed herewith. If the deficiencies indicated are not rectified the application may be refused pursuant to Article 97(2) EPC.

You are invited to file your observations and insofar as the deficiencies are such as to be rectifiable, to correct the indicated deficiencies within a period

of 4 months

from the notification of this communication, this period being computed in accordance with Rules 126(2) and 131(2) and (4) EPC. One set of amendments to the description, claims and drawings is to be filed within the said period on separate sheets (R. 50(1) EPC).

If filing amendments, you must identify them and indicate the basis for them in the application as filed. Failure to meet either requirement may lead to a communication from the Examining Division requesting that you correct this deficiency (R. 137(4) EPC).

In case you withdraw the application within the above-mentioned period, the examination fee will be refunded at a rate of 50% (Art. 11 (b) RFees).

Failure to comply with this invitation in due time will result in the application being deemed to be withdrawn (Art. 94(4) EPC).

Registered letter

EPO Form 2001 11.16TRI



Dingel, Janis
Primary Examiner
For the Examining Division

Enclosure(s): 4 page/s reasons (Form 2906)



Application No.: 14791882.5

Substantive examination has started on 29.11.17 (see Notice from the European Patent Office dated 29.01.2013, OJ EPO 2013, 153).

For the Examining Division

EP Application No.: 14 791 882.5
Applicant: WEBROOT INC.
Our Ref.: EP103926EH206
Date: June 9, 2017

CLAIMS

1. A method comprising:

gathering one or more events (504A-520A; 1208) defining an action of a first object (1232) acting on a target (1236);

generating a contextual state (524; 1216) for at least one of the one or more events by correlating (912) 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 (1244) on which the first object is executed and a user (1248) associated with the first object;

obtaining a global perspective for the at least one event by obtaining information (228; 528-536) associated with one or more of the first object and the originating object, the information including at least one of age (1260), popularity (1264), a determination (1268) 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 (1272);

assembling (624) an event line (244A-B) 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 (628) the assembled event line.

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

wherein the event line is transmitted to an end recipient (220).

3. The method of claim 1 or 2, further comprising:

obtaining (1112) 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 any one of claims 1 to 3, 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; and/or

further comprising:

determining (1008) 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 (1020) 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 (1016) a global perspective for the at least one event from a community database.

5. The method of claim 4, further comprising:

determining (1012) 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 (1016) a global perspective for the at least one event from a community database; and/or

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 (1260) of the first object; and a number of concurrent connections associated with the first object.

6. A computer readable storage medium comprising processor executable instructions operable to perform the method of any one of claims 1 to 5.

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

a device (204) including:

a communication interface (332);

a processor (316);

data storage (320); and

a sensor agent (208) stored on the data storage that is executable by the processor, wherein the sensor agent is operable to:

gather one or more events (504A-520A; 1208) defining an action of a first object (1232) acting on a target (1236);

generate a contextual state (524; 1216) for at least one of the one or more events by correlating (912) 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 (1244) on which the first object is executed and a user (1248) associated with the first object;

assemble (624) an event line (244A-B) 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 (628) the assembled event line utilizing the communication interface.

8. The system of claim 7, further comprising a global perspective information server (216) including:

a processor (464);

a communication interface (468);

data storage (488); and

a global perspective module (476), 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 (228; 528-536) associated with one or more of the first object and the originating object, the information including at least one of age (1260), popularity (1264), a determination (1268) 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 (1272);

assemble (624) 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 (628) the assembled second event line utilizing the communication interface to an end recipient (220).

9. The system of claim 7 or 8, 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 (1260) of the first object; and a number of concurrent connections associated with the first object; and/or

further comprising a bridge (222) including:

a processor (382);

a communication interface (386); and

a cached event store (394), 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 (228; 528-536) associated with one or more of the first object and the originating object, the information including at least one of age (1260), popularity (1264), a determination (1268) 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 (1272);

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.

10. The system of claim 7, wherein the sensor agent is further operable to:

obtain a global perspective for the at least one event by obtaining information (228) associated with one or more of the first object and the originating object, the information including at least one of age (1260), popularity (1264), a determination (1268) 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 (1272).
11. The system of claim 10, wherein the at least one of the one or more events is executed by the processor.
12. The system of claim 10 or 11, further comprising:

a global perspective information server (216); and

an end recipient device (220), 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.
13. The system of any one of claims 10 to 12, wherein the at least one event includes information uniquely identifying the object performing the action, information uniquely identifying the action being performed, and information uniquely identifying the target upon which the act is being performed.
14. The system of any one of claims 10 to 13, wherein the sensor agent is one or more of:

further operable to:

determine (1008) 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 (1020) 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 (1016) a global perspective for the at least one event from a community database; or

further operable to:

determine (1012) 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 (1016) a global perspective for the at least one event from a community database; or

further operable to:

cache the one or more events, and

asynchronously consolidate and normalize (816) the one or more events.

15. 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 (1260) of the first object; and a number of concurrent connections associated with the first object.

EP Application No.: 14 791 882.5
Applicant: WEBROOT INC.
Our Ref.: EP103926EH206
Date: June 9, 2017

CLAIMS (marked-up version)

1. A method comprising:
 - gathering one or more events (504A-520A; 1208) defining an action of a first object (1232) acting on a target (1236);
 - generating a contextual state (524; 1216) for at least one of the one or more events by correlating (912) 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 (1244) on which the first object is executed and a user (1248) associated with the first object;
 - obtaining a global perspective for the at least one event by obtaining information (228; 528-536) associated with one or more of the first object and the originating object, the information including at least one of age (1260), popularity (1264), a determination (1268) as to whether the first object is malware, a determination as to whether the originating object is malware; and Internet Protocol₁ {IP₁} Address or Uniform Resource Locator₁ {URL₁} information (1272);
 - assembling (624) an event line (244A-B) 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 (628) the assembled event line.
2. The method of claim 1, wherein the information associated with the one or more of the first object and the originating object is obtained from a community database; and
 - wherein the event line is transmitted to an end recipient (220).
3. The method of claim 1 or 2, further comprising:
 - obtaining (1112) 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 any one of claims 1 to 3, 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; and/or

further comprising:

determining (1008) 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 (1020) 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 (1016) a global perspective for the at least one event from a community database.

5. The method of claim 4, further comprising:

determining (1012) 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 (1016) a global perspective for the at least one event from a community database; and/or

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 (1260) of the first object; and a number of concurrent connections associated with the first object.

6. A computer readable storage medium comprising processor executable instructions operable to perform the method of any one of claims 1 to 5.

~~7-10. A system of claim 7, for providing forensic visibility into a system, comprising:
a device including:~~

~~a communication interface;~~

~~a processor;~~

~~data storage; and~~

~~a wherein the sensor agent stored on the data storage that is executable by the processor, wherein the sensor agent is further 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 (228) associated with one or more of the first object and the originating object, the information including at least one of age (1260), popularity (1264), a determination (1268) as to whether the first object is malware, a determination as to whether the originating object is malware; and Internet Protocol₁ (IP₁) Address or Uniform Resource Locator₁ (URL₁) information (1272);~~

~~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.~~

~~8.11.~~ The system of claim ~~7~~10, wherein the at least one of the one or more events is executed by the processor.

~~9.12.~~ The system of claim ~~7~~10 or ~~8~~11, further comprising:

a global perspective information server (216); and

an end recipient device (220), 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.

~~40.13.~~ The system of any one of claims ~~710~~ to ~~912~~, 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.

~~44.14.~~ The system of any one of claims ~~710~~ to ~~4013~~, wherein the sensor agent is one or more of:

further operable to:

determine (1008) 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 (1020) 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 (1016) a global perspective for the at least one event from a community database; or

further operable to:

determine (1012) 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 (1016) a global perspective for the at least one event from a community database; or

further operable to:

cache the one or more events, and

asynchronously consolidate and normalize (816) the one or more events.

~~42.15.~~ The system of claim ~~4013~~, 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 (1260) of the first object; and a number of concurrent connections associated with the first object.

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

a device (204) including:

a communication interface (332);

a processor (316);

data storage (320); and

a sensor agent (208) stored on the data storage that is executable by the processor, wherein the sensor agent is operable to:

gather one or more events (504A-520A; 1208) defining an action of a first object (1232) acting on a target (1236);

generate a contextual state (524; 1216) for at least one of the one or more events by correlating (912) 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 (1244) on which the first object is executed and a user (1248) associated with the first object;

assemble (624) an event line (244A-B) 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 (628) the assembled event line utilizing the communication interface.

14.8. The system of claim 43.7, further comprising a global perspective information server (216) including:

a processor (464);

a communication interface (468);

data storage (488); and

a global perspective module (476), 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 (228; 528-536) associated with one or more of the first object and the originating object, the information including at least one of age (1260), popularity (1264), a determination (1268) as to whether the first object is malware, a determination as to whether the originating object is malware; and Internet Protocol₁ {IP₁} Address or Uniform Resource Locator₁ {URL₁} information (1272);

assemble (624) 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 (628) the assembled second event line utilizing the communication interface to an end recipient (220).

45.9. The system of claim 437 or 448, 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 (1260) of the first object; and a number of concurrent connections associated with the first object; and/or

further comprising a bridge (222) including:

a processor (382);

a communication interface (386); and

a cached event store (394), 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 (228; 528-536) associated with one or more of the first object and the originating object, the information including at least one of age (1260), popularity (1264), a determination (1268) as to whether the first object is malware, a determination as

to whether the originating object is malware; and Internet Protocol₁ (IP₁) Address or Uniform Resource Locator₁ (URL₁) information (1272);

obtain a second global perspective for the another event;

provide the first global perspective to the device; and

provide the second global perspective to the another device.

~~METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO
SYSTEMS AND NETWORKS~~~~CROSS-REFERENCE TO RELATED APPLICATIONS~~

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,
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
20 disk or to a database over the network.

However, existing network forensic tools, such as network sniffers and packet
capturing tools, passively collect information about network traffic. Such tools may be
able to detect and capture information associated with communication sessions, such as
hostnames, ports, protocols, IP addresses, etc.; however, such tools tend to receive
25 network events outside of a host or system. That is, a network forensic tool, such as a
network sniffer, may reside at a network edge and may receive network events concerning
the network from one or more hosts or systems. Accordingly, network edge devices have
no ability to establish any sort of context from within the host or system that is generating
the event. Therefore, devices residing at a network edge may monitor, record, and or
30 analyze network traffic between the host and the device, but information that may be
useful within the host is not obtained.

For example, Figure 1 generally illustrates a comparative example including
computing devices 104 and 108 in communication with a network edge device 116. The
network edge device 116 may be commonly referred to as a “sniffer” which may monitor,

capture, and analyze network traffic between the network edge device 116 and the computing devices 104 and 108. The network edge device 116 may further be in communication with a communication network 124, such as the internet. Accordingly, the network edge device 116 may monitor, capture, and analyze network traffic between the computing devices 104 and 108 and between the computing devices 104/108 and the communication network 124.

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

SUMMARY

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

WO 2012/110501 A1 relates to methods and apparatus for dealing with malware. In one aspect, a method of classifying a computer object as malware includes at a base computer (3), receiving data about a computer object from each of plural remote computers (2) on which the object or similar objects are stored and or processed. The base computer (3) comprises plural threat servers (62) arranged to receive said data from the plural remote computers (2) and apply rules and or heuristics against that data in real time to determine whether or not said object is malware and to communicate said determination to the remote computers (2). The base computer (3) comprises at least one central server (74) in communication with the threat servers (62) and arranged to receive said data about objects from the threat servers (62) to maintain a master database (71, 72, 73) of data received about objects from all of the threat servers (62).

US 2008/244694 A1 relates to the automated collection of forensic evidence associated with a network security incident. An automated collection of forensic evidence associated with a security incident is provided by an arrangement in which different security products called endpoints in an enterprise network are enabled for sharing security-related information over a common communication channel using an abstraction called a security assessment. A security assessment is generally configured to indicate an endpoint's understanding of a detected security incident that pertains to an object in the environment which may include users, computers, IP addresses, and website URIs (Universal Resource Identifiers). The security assessment is published by the endpoint into the channel and received by subscribing endpoints. The security assessment triggers the receiving endpoints to go into a more comprehensive or detailed mode of evidence collection. In addition, any forensic evidence having relevance to the security incident that may have already been collected prior to the detection will be marked for retention so that it is not otherwise deleted.

SUMMARY

It is the object of the present invention to provide an improved method for providing forensic visibility into systems and networks, as well as a corresponding system and computer readable medium.

This object is solved by the subject matter of the independent claims.

Preferred embodiments are defined by the dependent claims.

~~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
5 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
10 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
15 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
20 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
25 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
30 implementation, six components, or modules, may be utilized in the event gathering and
processing: low level system filters, a local aggregator and interpreter, a context analyzer,
a global perspective module, an event priority module, and an event distributor may be
utilized to provide forensic visibility into one or more computing devices of a
communication network.

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

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

09. Juni 2017

Grünecker PartG mbB Leopoldstr. 4 80802 München Germany

European Patent Office

Bob-van-Benthem-Platz 1
80469 München

Ihr Zeichen / Your Ref.

Unser Zeichen / Our Ref.

Datum / Date

EP103926EH206amr

June 9, 2017

European Patent Application No. 14 791 882.5
Applicant: WEBROOT INC.

In response to the Official Communication under Rules 70(2) and 70a (2) EPC
dated November 29, 2016:

- I. The above-mentioned European patent application is to be further prosecuted.
- II. In reply to the deficiencies noted in the European Search Opinion, submitted herewith are:
 - new claims 1 to 15 to replace all claims presently on file; and
 - new description pages 1, 2, 2a, 2b and 3 to replace description pages 1, 2 and 3 presently on file.

Also enclosed is a marked-up version of the new claim set, highlighting all claim amendments.

The claims and description have been amended in order to overcome all objections raised in the above-mentioned Official Communication.

I. Amendments and Clarity

New claims 1 to 6 correspond to original claims 1 to 6, respectively.

Grünecker Patent- und Rechtsanwälte PartG mbB

Leopoldstr. 4
80802 München
Germany

Tel. +49 (0) 89 21 23 50
Fax +49 (0) 89 22 02 87
Mail info@grunecker.de

Amtsgericht: München
Partnerschaftsregister:
PR 1397

Deutsche Bank München
SWIFT / BIC-code: DEUT DE MM
IBAN: DE 47 7007 0010 0175 173400

¹ auch/also: Mediator ² auch/also: Agente de la Propriété Industrielle (España) ³ auch/also: Consulente in Brevetti (Italia)
⁴ Professor an der Fachhochschule für angewandtes Management ⁵ auch/also: Attorney-at-Law, New York ⁶ in Kooperation/in cooperation

MÜNCHEN

Patentanwälte **European Patent Attorneys**

Hans Hilgers
Thomas Schuster
Dr. Klara Goldbach
Martin Aufenanger, LL.M., MM.¹
Gottfried Klitzsch
Dr. Heike Vogelsang-Wenke
Reinhard Knauer
Dietmar Kuhl
Dr. Franz-Josef Zimmer
Bettina K. Reichelt
Dr. Anton K. Pfau
Dr. Udo Weigelt, LL.M.
Rainer Bertram
Jens C. Koch, M.S. (U of PA)
Bernd Rothaemel
Thomas W. Laubenthal, LL.M.
Dr. Andreas Kayser
Dr. Jens Hammer
Dr. Thomas Eickelkamp
Dr. Peter Miltényi²
Dr. Moritz Höffe, LL.M.
Gero Maatz-Jansen
Michael Heise
Christian Meisinger
Dr. Martin Ahr
Dr. Wolfgang Neubeck
Steven M. Zeman, Ph.D.
André Nickel
Felix Kahr
Dr. Alexander Stumvoll, LL.M.
Dr. Stefano Marchini³
Dr. Thomas Kronberger
Yilin Jin
Dr. Georg Seisenberger
Amir Nemetzade
Dr. Olivia Nemethova, LL.M.
Dr. Rainer Plaggenborg
Victor Lopes Aguiar

Rechtsanwälte **Attorneys-at-Law**

Dr. Helmut Eichmann
Gerhard Barth
Dr. Ulrich Blumenröder, LL.M.
Prof. Dr. Maximilian Kinkeldey, LL.M.⁴
Dr. Karsten Brandt
Anja Franke, LL.M.
Ute Stephani
Dr. Bernd Allekotte, LL.M.⁵
Dr. Elvira Bertram, LL.M.
Babett Ertle
Christine Neuhierl
Sabine Brandstätter
Cornelia Schmitt
Petra Lübke
Dr. Holger Gauss
Dr. Nicolás Schmitz
Marina Schlumberger
Kirsten Hammerstingl
Sebastian Clotten, LL.M.
Jennifer Rosenhäger, LL.M.
Mark Peters, LL.M.
Dr. Nicola Busch
Julia Bittner, LL.M.
Sebastian Ochs
Philipp Strommer
Jan Rether

BERLIN

Patentanwälte **European Patent Attorneys**

Dr. Patrick P. Erk, M.S. (MIT)
Dr. Svenja Sethmann
Tino Rumpold

KÖLN

Patentanwälte **European Patent Attorneys**

Dr. Martin Droppmann

PARIS⁶

Conseil en Propriété Industrielle
European Patent Attorney
Dr. Wolfgang Neubeck

New claims 7 to 9 correspond to original claims 13 to 15, respectively.

New dependent claim 10 is based on original independent claim 7 and has been redrafted as a dependent claim on new claim 7.

New claims 11 to 15 correspond to original claims 8 to 12, respectively.

Accordingly, the claims do not introduce subject matter extending beyond the content of the application as originally filed and fulfill the requirements of Article 123(2) EPC.

As the new claim set comprises a single independent claim per claim category, the objection raised under **Section 1** of the Official Communication is considered to be overcome.

The independent claims have been drafted in the one-part form, as introducing the two-part form against the disclosure of the closest prior art would require an unduly complex claim wording, which would render the subject matter more difficult to comprehend. Therefore, the one-part form is considered more pertinent and allowable in this case, as provided for under Rule 43(1) EPC. In this regard, it should also be noted that the closest prior art D1 has been acknowledged in the opening part of the description in accordance with European patent practice, so that a skilled person can understand the differences and the contribution of the claimed invention over the closest prior art.

Description pages 1 and 3 have been amended as requested under **item 3.4** of the Official Communication.

Reference signs have been introduced into the claims where possible and appropriate, as requested under **items 3.5** and **3.6** of the Official Communication.

With the new description pages 2, 2a and 2b as submitted, the description has been brought into conformity with the new claims, as requested under **item 3.7** of the Official Communication.

Moreover, cited prior art documents D1 and D2 have been identified and briefly acknowledged in the opening part of the description, as requested under **item 3.8** of the Official Communication.

II. Patentability

The Examining Division's arguments and analysis concerning the cited prior art documents are highly appreciated and have been carefully considered and taken into account. However, in regard to the new claims, the Examining Division is kindly requested to consider the following arguments, which lead to the conclusion that the claimed subject matter is novel and involves an inventive step over the available prior art.

In particular, D1 relates to methods and apparatus for dealing with malware. In one aspect, a method of classifying a computer object as malware includes at a base computer (3), receiving data about a computer object from each of plural remote computers (2) on which the object or similar objects are stored and or processed. The base computer (3) comprises plural threat servers (62) arranged to receive said data from the plural remote computers (2) and apply rules and or heuristics against that data in real time to determine whether or not said object is malware and to communicate said determination to the remote computers (2). The base computer (3) comprises at least one central server (74) in communication with the threat servers (62) and arranged to receive said data about objects from the threat servers (62) to maintain a master database (71, 72, 73) of data received about objects from all of the threat servers (62).

In contrast, according to the claimed invention,

- (1) one or more events are gathered, each defining an action of a first object acting on a target.
- (2) a contextual state (including a device, a user and an originating object) is generated for an event by correlating the event to an originating object,
- (3) A global perspective (including age, popularity, whether the first/originating object is malware, and IP/URL information) is obtained for the event by obtaining information associated with the first object and the originating object,
- (4) An event line is assembled including details of the event (first/originating object, target, action) and the event line is transmitted.

Thus, it is respectfully submitted that D1 fails to disclose many of the core features of the claimed invention. In particular, it can be understood from the Official Communication that the Examining Division is of the opinion that gathering one or more events would

correspond to collecting metadata about the object in D1, including events data that define the actions or behaviors of an object acting upon another object or some entity. Further, the Examining Division seems to be of the opinion that generating a contextual state by correlating the event to an originating object, the contextual state including an indication of the originating object, would correspond to the metadata in D1 also including a Genesisactor which is the key of an object that is the ultimate parent of the event being performed.

In this regard, it is respectfully pointed out that although D1 suggests that the metadata (i.e. the contextual state as alleged by the Examining Division) includes a Genesisactor (i.e. originating object as suggested by the Examining Division), D1 does not disclose that the contextual state (metadata) is generated by correlating the event to the originating object (Genesisactor).

In D1 the event data is not correlated with an originating object to generate the metadata because the event data is part of the metadata. In other words, the metadata of D1 cannot correspond to the contextual state as alleged by the Examining Division as it is not generated by correlating the event with an originating object. Moreover, it is respectfully pointed out that page 39 of D1, lines 3 to 12 seems to suggest that the identity of the remote computer and the creator of the file are separate from the metadata, and thus cannot correspond to a contextual state for the event included in the metadata.

Moreover, it can be understood from the Official Communication that the Examining Division is of the opinion that obtaining a global perspective for the event would correspond to receiving from the base computer 3 determinations of whether the objects are safe or not. In this regard, it is respectfully submitted that D1 is silent regarding obtaining a global perspective for the event. In other words, although some information for the object is received in D1, this information is not obtained for an event. In particular, as discussed in detail below, while the claimed invention is directed at obtaining information such as contextual state and a global perspective that would provide an insight about an event (including information about objects), D1 is directed at obtaining detailed information regarding an object (possibly including information about some events), which is different.

It can be further understood that the Examining Division is of the opinion that assembling an event line and transmitting the event line is anticipated by Figure 10 of D1. In this regard, it is respectfully submitted that no passage in D1 suggests assembling an event line, let alone transmitting such an event line. Although some event data including

information about an actor, an event type and a victim is part of the metadata of an object, D1 does not suggest assembling an event line. Moreover, it is respectfully pointed out that the Genesisactor data seems to be separate from the event data in D1.

Furthermore, it is respectfully submitted that Figure 10 of D1 displays a table in which the rows represent the objects that match the results of a current query. As such, D1 would, if at all, suggest some kind of an object line, and not an event line.

It is further submitted that while the claimed invention deals with events as the main entity, and assembles additional information regarding the events (contextual state, and global perspective) into an event line, D1 deals with objects as the main entity for the analysis. In other words, according to the claimed invention the details are gathered for an event, while in D1 the details are gathered for the objects. As such, it is respectfully submitted that the claimed invention provides a different solution for providing forensic visibility that is not suggested by D1.

Similarly, this scheme is not suggested by D2. D2 relates to the automated collection of forensic evidence associated with a network security incident. An automated collection of forensic evidence associated with a security incident is provided by an arrangement in which different security products called endpoints in an enterprise network are enabled for sharing security-related information over a common communication channel using an abstraction called a security assessment. A security assessment is generally configured to indicate an endpoint's understanding of a detected security incident that pertains to an object in the environment which may include users, computers, IP addresses, and website URIs (Universal Resource Identifiers). The security assessment is published by the endpoint into the channel and received by subscribing endpoints. The security assessment triggers the receiving endpoints to go into a more comprehensive or detailed mode of evidence collection. In addition, any forensic evidence having relevance to the security incident that may have already been collected prior to the detection will be marked for retention so that it is not otherwise deleted.

Thus, it is respectfully submitted that while D2 suggests that security assessments are shared among SEs, which enables the SEs to combine and correlate evidence from security assessments received from a variety of sources, and across object types, it does not disclose the aforementioned scheme of the claimed invention.

In particular, the security assessment in D2 includes information that is collected about an object such as computer, user, service, external IP address, data etc, along with an assessment category and the severity of the detected incident. However, D2 fails to disclose many of the core features of the claimed invention such as at least correlating an event with an originating object to generate a contextual state, or assembling an event line including information uniquely identifying each of the first object, the action of the first object, the target, and the originating object.

Since neither D1 nor the remaining prior art disclose or suggest the aforementioned distinguishing features, the claimed subject matter does not arise from the available prior art in an obvious manner, but involves an inventive step within the meaning of Article 56 EPC.

In view of the above, it is the object of the claimed invention to provide an improved method for providing forensic visibility into systems and networks, as well as a corresponding system and computer readable medium.

This object is solved by the present invention and specifically by the above-discussed distinguishing features of the subject matter of the independent claims.

Consequently, the new claims are considered allowable under Article 52 EPC.

III. Summary

The Examining Division is kindly requested to proceed with the examination proceedings based on the new claims and arguments submitted in response to the deficiencies noted in the Search Opinion. As a precautionary measure, oral proceedings are herewith requested for the examination proceedings.



M. Heise

Encl.

Claims 1 to 15 (clean and marked-up versions)
Description pages 1, 2, 2a, 2b and 3



European Patent Office
80298 MUNICH
GERMANY

Questions about this communication ?
Contact Customer Services at www.epo.org/contact



Grünecker Patent- und Rechtsanwälte
PartG mbB
Leopoldstraße 4
80802 München
ALLEMAGNE

Date
29.11.16

Reference EP103926EHjet	Application No./Patent No. 14791882.5 - 1870 / 2992471 PCT/US2014036832
Applicant/Proprietor Webroot Inc.	

Communication pursuant to Rules 70(2) and 70a(2) EPC

A supplementary European search report has been drawn up concerning the above-identified European patent application (publication number: 2992471).

Since the request for examination has been filed (R. 70(1), 159(1)(f), Art. 94(1) EPC) prior to the transmission of the supplementary European search report, you are hereby invited to indicate within

six months

of notification of this communication whether you wish to proceed further with the European patent application.

If you do not indicate in due time that you wish to proceed further with the European patent application, it **will be deemed to be withdrawn** (R. 70(3) EPC).

You are invited, within the above-mentioned six-month period, to comment on the objections raised in the opinion accompanying the European search report and/or to file any amendments to the description, claims and drawings correcting any deficiencies noted in the opinion (R. 70a(2), R. 137(2) EPC; Guidelines for Examination in the EPO, B-XI, 8).

If filing amendments, you must identify them and indicate the basis for them in the application as filed. Failure to meet either requirement may lead to a communication from the Examining Division requesting that you correct this deficiency (R. 137(4) EPC).

Should the reply to the invitation pursuant to Rule 70a(2) EPC be filed in an admissible non-EPO language, a translation is to be submitted within one month of its filing (R. 6(2) EPC).

Should you not comply with this invitation within the time limit, the application **will be deemed to be withdrawn** in accordance with Rule 70a(3) EPC.

Receiving Section



Registered letter
EPO Form 1224 11.12 (RTB/ESOP01=N) DMEX

Page: 1 of 1



European Patent Office
80298 MUNICH
GERMANY

Questions about this communication ?
Contact Customer Services at www.epo.org/contact



Grünecker Patent- und Rechtsanwälte
PartG mbB
Leopoldstraße 4
80802 München
ALLEMAGNE

Date
11.11.16

Reference EP103926EHjet	Application No./Patent No. 14791882.5 - 1870 / 2992471 PCT/US2014036832
Applicant/Proprietor Webroot Inc.	

Communication

The extended European search report is enclosed.

The extended European search report includes, pursuant to Rule 62 EPC, the supplementary European search report (Art. 153(7) EPC) and the European search opinion.

Copies of documents cited in the European search report are attached.

☒ 0 additional set(s) of copies of such documents is (are) enclosed as well.

Refund of the search fee

If applicable under Article 9 Rules relating to fees, a separate communication from the Receiving Section on the refund of the search fee will be sent later.

Should you wish to further prosecute this application in the examination phase, your attention is drawn to the provisions of Rule 70a EPC. An invitation to respond to the extended European search report will be issued shortly (R. 70(2) EPC).



The examination is being carried out on the **following application documents**

Description, Pages

1-34 as published

Claims, Numbers

1-15 as published

Drawings, Sheets

1/15-15/15 as published

Reference is made to the following documents; the numbering will be adhered to in the rest of the procedure.

- D1 WO 2012/110501 A1 (PREVX LTD [GB]; MORRIS MELVYN [GB]; JAROCH JOSEPH [US]) 23 August 2012 (2012-08-23)
- D2 US 2008/244694 A1 (NEYSTADT JOHN [IL] ET AL) 2 October 2008 (2008-10-02)
- D3 WO 2006/094228 A2 (MARKMONITOR INC [US]; SHULL MARK [US]; BOHLMAN WILLIAM [US]; SHRAIM IH) 8 September 2006 (2006-09-08)

1 Conciseness (Article 84 EPC)

- 1.1 The application does not meet the requirements of Article 84 EPC, because claims 7 and 13 are not concise.

Claims 7 and 13 have been drafted as separate independent claims.

Under Article 84 in combination with Rule 43(2) EPC, an application may contain more than one independent claim in a particular category only if the subject-matter claimed falls within one or more of the exceptional situations set out in paragraph (a), (b) or (c) of Rule 43(2) EPC. This is not the case in the present application, however, for the following reason: the subject-matter of claim 7 includes all features of claim 13 and should be formulated as a dependent claim.

2 Novelty and Inventive Step (Article 54 and 56 EPC)

2.1 The present application does not meet the requirements of Article 52(1) EPC because the **subject-matter of claim 1** is not new within the meaning of Article 54(1) and (2) EPC. Document D1 discloses (references in parentheses applying to this document):

A method comprising:

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

(p.21, l.28-32: "Amongst other types, the types of metadata captured and sent to the base computer 3 might be: "Events": these define the actions or behaviours of an object acting upon another object or some other entity")

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

(p.21, l.28 - p.22, l.24: [...] metadata captured [...] might be: [...] "Genesisactor": the key of an object that is not the direct Actor of an event but which is the ultimate parent of the event)

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;

(p.39, l.3: "The table 105 has a plurality of columns of data representing information about the objects [...]. [...] the identity of the remote computer that encountered the object, [...], the creator of the file [...]")

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,

(p.24, l.20-26: "In short, the agent program 10 [~~the~~] monitors objects on that computer 2 and their behaviour and communicates with the base computer 3 to send details of new objects and behaviour found on the remote computer 2 and to receive determinations of whether the objects are safe or not."; Fig. 3)

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;

(claim 1: "[...] at a base computer, receiving data about a computer object from each of plural remote computers [...] and apply rules and or heuristics

against that data in real time to determine whether or not said object is malware and to communicate said determination to the remote computers [...]"

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

(p.29, l.18-20: "The location of the remote computer can be determined by any convenient means, such as examining the IP address")

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.

(Fig. 10: assembling of object information, querying and displaying to users)

- 2.2 It may also be noted that the subject-matter of claim 1 is not inventive over D2 disclosing a security assessment system with distributed management of security incidents (D2, Fig. 1, para [0018]). Security assessment endpoints perform logging of local actions (see [0019]). An assessment sharing manager provides a global security perspective by sharing security assessments within the system (Fig. 2, (242); [0038]). Enabling an endpoint to correlate evidence from security assessments received from a variety of different sources ([0017]).
- 2.3 The subject-matter of independent claims 6, 7 and 13 corresponds in terms of apparatus features or computer program to that of claim 1. The objections raised in respect of this latter claim, therefore, also apply to independent claims 6, 7 and 13, which is thus not allowable under Article 54 EPC.
- 2.4 The additional features of the dependent claims 2,4,5,8,9,10,11,12,14 and 15 do not add anything new or inventive to the independent claims, because these features are known from the above mentioned prior art D1 (claim 2: community database (Fig.1 (7), p.18, l.16: "When the community database 7 is searched for the signature of the object that was not previously known"); claim 4, 10 and 11: uniquely identifying (p.21-p.23) and local or global cache (p.18,l.4: "If the object is still not classified locally, then details of the object are passed over the Internet 1 or other network to the base computer 3 for storing in the community database 7 and preferably for further analysis at the base computer 3"); claim 5, 12 and 15: displaying (Fig. 10); claim 9, 14: global perspective information server (Fig. 3, base computer (3))).

- 2.5 Claim 3 (obtaining event priority) is not inventive in combination with document D2. Document D2 disclosing assigning a severity level to a detected incident as part of security assessment (D2, [0015]).
- 2.6 Features related to the determination whether a local cache has expired (claim 11) are not inventive in combination with document D3 from the same technical field, disclosing an agent for monitoring network activity and assigning trust scores to online entities (D3, Fig. 1). Trust scores are cached in a local trust cache (D3, [0086]). Cache entries may expire after a predetermined time (D3, [0093-0094]) requiring the monitoring agent to fetch updates from a trust score server.

3 Further remarks

- 3.1 If the applicant intends to proceed further with the present application and is of the opinion that the application does in fact contain subject-matter that could support a patentable claim, then a new independent claim should be filed, setting out what is considered to be the inventive contribution to the art.
- 3.2 In his letter of reply the applicant should clearly indicate the parts of the originally filed application serving as a basis for subject-matter newly introduced into the claims. This would greatly facilitate the subsequent substantive examination of the claims with respect to Article 123(2) EPC.
- 3.3 Any new independent claim should be in the two-part form recommended by Rule 43(1) EPC having a pre-characterising portion which correctly reflects the prior art of the cited document D1.
- 3.4 The "incorporated by reference" statement on pp. 1 and 3 should be deleted, in accordance with the Guidelines for Examination, part F-III, 8.
- 3.5 In the claims, parentheses are to be used exclusively for reference signs Rule 43(7) EPC.
- 3.6 In the claims, the reference signs from the drawings relating to technical features should be introduced in parentheses, Rule 43(7) EPC.
- 3.7 The opening part of the description should be modified to bring it into agreement with any amended independent claims, Rule 42(1)(c) EPC.
- 3.8 To meet the requirements of Rule 42(1)(b) EPC, the documents D1 and D2 should be acknowledged and briefly discussed in the opening part of the description.

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

APPLICANT: Webroot Inc.

IPC CLASSIFICATION: G06F21/00, G06F21/56, H04L29/06

EXAMINER: Dingel, Janis

CONSULTED DATABASES: WPI, ANSERA, DOSYS, EPODOC

CLASSIFICATION SYMBOLS DEFINING EXTENT OF THE SEARCH:

IPC:

CPC: G06F21/56, H04L63/14

FI/F-TERMS:

KEYWORDS OR OTHER ELEMENTS FEATURING THE INVENTION:
ICT

**SUPPLEMENTARY
EUROPEAN SEARCH REPORT**

Application Number
EP 14 79 1882

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	WO 2012/110501 A1 (PREVX LTD [GB]; MORRIS MELVYN [GB]; JARACH JOSEPH [US]) 23 August 2012 (2012-08-23)	1,2,4-15	INV. G06F21/00 G06F21/56 H04L29/06
Y	* page 16, line 15 - page 27, line 25 * * page 38, line 21 - page 41, line 2 * * page 44, line 5 - line 20; claim 1; figures 1,3,10 *	3	
X	US 2008/244694 A1 (NEYSTADT JOHN [IL] ET AL) 2 October 2008 (2008-10-02)	1,6,7,13	
Y	* paragraph [0015] - paragraph [0019] *	3	
A	* paragraph [0034] * * paragraph [0038] * * paragraph [0042] - paragraph [0046] * * paragraph [0053] - paragraph [0058]; figures 1-3 *	2,4,5, 8-12,14, 15	
A	WO 2006/094228 A2 (MARKMONITOR INC [US]; SHULL MARK [US]; BOHLMAN WILLIAM [US]; SHRAIM IH) 8 September 2006 (2006-09-08) * paragraph [0083] - paragraph [0086]; figure 1 * * paragraph [0093] - paragraph [0094] * * paragraph [0102] *	11	TECHNICAL FIELDS SEARCHED (IPC) G06F H04L
The supplementary search report has been based on the last set of claims valid and available at the start of the search.			
Place of search Munich		Date of completion of the search 2 November 2016	Examiner Dingel, Janis
CATEGORY OF CITED DOCUMENTS X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document			

2
EPO FORM 1503 03.82 (P04C04)

**ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.**

EP 14 79 1882

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report.
The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

02-11-2016

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2012110501 A1	23-08-2012	AU 2012217181 A1	05-09-2013
		CA 2827385 A1	23-08-2012
		CN 103493061 A	01-01-2014
		CN 105868635 A	17-08-2016
		EP 2676219 A1	25-12-2013
		EP 2750070 A2	02-07-2014
		EP 2750071 A2	02-07-2014
		HK 1199521 A1	03-07-2015
		HK 1199522 A1	03-07-2015
		JP 5967107 B2	10-08-2016
		JP 2014509007 A	10-04-2014
		US 2012260304 A1	11-10-2012
		US 2012260340 A1	11-10-2012
		US 2012266208 A1	18-10-2012
		US 2014304800 A1	09-10-2014
		WO 2012110501 A1	23-08-2012
US 2008244694 A1	02-10-2008	EP 2142996 A1	13-01-2010
		EP 2143033 A2	13-01-2010
		US 2008244694 A1	02-10-2008
		US 2008244742 A1	02-10-2008
		US 2008244748 A1	02-10-2008
		WO 2008122058 A2	09-10-2008
		WO 2008124295 A1	16-10-2008
WO 2006094228 A2	08-09-2006	WO 2009005925 A2	08-01-2009
		CA 2600344 A1	08-09-2006
		CA 2600373 A1	08-09-2006
		EP 1856639 A2	21-11-2007
		EP 1856640 A2	21-11-2007
		US 2006212925 A1	21-09-2006
		US 2006212930 A1	21-09-2006
		US 2006212931 A1	21-09-2006
		WO 2006094228 A2	08-09-2006
		WO 2006094271 A2	08-09-2006
		WO 2006094275 A2	08-09-2006

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82



Application No.: 14791882.5

The search has started on 29.09.16 (see Notice from the European Patent Office dated 03/2013, OJ EPO 2013, 153).

Receiving Section



European Patent Office
80298 MUNICH
GERMANY

Questions about this communication ?
Contact Customer Services at www.epo.org/contact



Grünecker Patent- und Rechtsanwälte
PartG mbB
Leopoldstraße 4
80802 München
ALLEMAGNE

Date
10.02.16

Reference EP103926EHjet	Application No./Patent No. 14791882.5 - 1853 / 2992471 PCT/US2014036832
Applicant/Proprietor Webroot Inc.	

Communication of European publication number and information on the application of Article 67(3) EPC

The provisional protection under Article 67(1) and (2) EPC in the individual Contracting States becomes effective only when the conditions referred to in Article 67(3) EPC have been fulfilled (for further details, see information brochure of the European Patent Office "National Law relating to the EPC" and additional information in the Official Journal of the European Patent Office).

Pursuant to Article 153(3) EPC the publication under Article 21 PCT of an international application for which the European Patent Office is a designated or elected Office takes the place of the publication of a European patent application.

The bibliographic data of the above-mentioned Euro-PCT application will be published on 09.03.16 in Section I.1 of the European Patent Bulletin. The European publication number is 2992471.

In all future communications to the European Patent Office, please quote the application number plus Directorate number.

Receiving Section





European Patent Office
80298 MUNICH
GERMANY

Questions about this communication ?
Contact Customer Services at www.epo.org/contact



Grünecker Patent- und Rechtsanwälte
PartG mbB
Leopoldstraße 4
80802 München
ALLEMAGNE

Date
20.01.16

Reference EP103926EHjet	Application No./Patent No. 14791882.5 - 1853 PCT/US2014036832
Applicant/Proprietor Webroot Inc.	

Communication pursuant to Rules 161(2) and 162 EPC

1. Amendment of the application (R. 161(2) EPC)

The above-mentioned international (Euro-PCT) application has entered the European phase.

Under Articles 28, 41 PCT and Rules 52, 78 PCT the application may be amended before a designated or elected Office.

In accordance with Rule 161(2) EPC, you may amend your application once within a **non-extendable period of six months** after notification of the present communication.

If filing amendments, you must identify them and indicate the basis for them in the application as filed. Failure to meet either requirement may lead to a communication from the Examining Division requesting that you correct this deficiency (R. 137(4) EPC).

The claims applicable on expiry of this period, i.e. those filed on entry into the European phase or in response to the present communication, will form the basis for the calculation of any claims fee to be paid (see page 2).

2 Claims fees under Rule 162 EPC

If the application documents on which the European grant procedure is to be based comprise more than fifteen claims, a claims fee shall be payable for the sixteenth and each subsequent claim within the period provided for in Rule 159(1) EPC.

- ☒ Based on the application documents currently on file, all necessary claims fees have already been paid (or the documents do not comprise more than 15 claims).
- ☐ All necessary fees will be debited automatically according to the automatic debit order.
- ☐ The claims fees due for the claims to were not paid within the above-mentioned period.

Registered letter
EPO Form 1226CC 06.15 (NFS) EUCL (13/01/16)

Any outstanding claims fee, either based on the current set of claims or on any amended claims to be filed pursuant to Rule 161 EPC (see page 1), may still be validly paid within a **non-extendable period of six months** after notification of this communication (R. 162(2) EPC).

If a payment is made for only some of the claims, you must indicate for which claims it is intended. If a claims fee is not paid in due time, the claim concerned is deemed to be abandoned (R. 162(4) EPC).

If claims fees have already been paid, but on expiry of the above-mentioned period there is a new set of claims containing fewer fee-incurring claims than before, the claims fees in excess of those due under Rule 162(2), second sentence EPC will be refunded (R. 162(3) EPC).

You are reminded that the supplementary search carried out according to Article 153(7) EPC will relate only to the last set of claims applicable on expiry of the above period AND will be confined to those fee-incurring claims for which fees have been paid in due time.

The claims fee is currently

**EUR 235 for the 16th and each subsequent claim up to the limit of 50
EUR 580 for the 51st and each subsequent claim**

Note to users of the automatic debiting procedure

Unless the EPO receives prior instructions to the contrary, the fees for all claims incurring fees will be debited on the last day of the period for payment. For further details see the Arrangements for the automatic debiting procedure, Annex A.1 to the ADA, Point 6.1(d), supplementary publication 3 - OJ EPO 2015.

Important information concerning fee amounts

Following any amendment to the Rules relating to Fees, the amount(s) mentioned in this communication may be different from the amount(s) **actually due on the date of payment**. The latest version of the Schedule of fees and expenses, published as a Supplement to the Official Journal of the EPO, is also available on the EPO website (www.epo.org) and can be found under www.epo.org/schedule-of-fees, which allows the viewing, downloading and searching for individual fee amounts, both current and previous.

Please note that procedural fees are usually adjusted every two years, on even years, with effect from 1 April.

Payments by cheque delivered or sent direct to the EPO are no longer accepted as from 1 April 2008 (see OJ EPO 2007, 626).

Receiving Section





European Patent Office
80298 MUNICH
GERMANY

Questions about this communication ?
Contact Customer Services at www.epo.org/contact



Grünecker Patent- und Rechtsanwälte
PartG mbB
Leopoldstraße 4
80802 München
ALLEMAGNE

Date
19.01.16

Reference EP103926EHjet	Application No./Patent No. 14791882.5 - 1853 PCT/US2014036832
Applicant/Proprietor Webroot Inc.	

Decision on the request for further processing under Rule 135(3) EPC

The request for further processing received on 22.12.15 has been granted (Art. 121(2) EPC).

- ☐ The legal consequence notified in the communication dated that the application was deemed to be withdrawn shall not ensue.
- ☒ The legal consequence shall not ensue.
- ☐ The refusal of the application dated shall not ensue.
- ☐ The legal consequence notified in the communication dated that the particular loss of rights occurred shall not ensue.
- ☐ The time limit set in the communication dated is deemed to have been met.

The procedure shall be continued/the particular loss of rights shall not ensue (Art. 121(3) EPC).

Important information in case of a PACE request

If a PACE request has been validly filed for the application, the applicant is herewith informed that the application is removed from the PACE programme. A second PACE request for that application during the same stage of the procedure will not be processed (see OJ EPO 2015, A93, point 4).

Receiving Section



Registered letter
EPO Form 1144 12.15 (NFS) (12/01/16)

RFPR4=3



European Patent Office
80298 MUNICH
GERMANY

Questions about this communication ?
Contact Customer Services at www.epo.org/contact



MAYR, Johannes
Lederergasse 31A
A-4020 Linz
AUTRICHE

Date
11.01.16

Reference	Application No./Patent No. 14791882.5 - 1853 PCT/US2014036832
Applicant/Proprietor Webroot Inc.	

Notification of the data mentioned in Rule 19(3) EPC

In the above-identified patent application you are designated as inventor/co-inventor.
Pursuant to Rule 19(3) EPC the following data are notified herewith:

DATE OF FILING : 05.05.14

PRIORITY : US/03.05.13/ USP201361819470

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

DESIGNATED STATES : AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE
IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM
TR

Receiving Section





European Patent Office
80298 MUNICH
GERMANY

Questions about this communication ?
Contact Customer Services at www.epo.org/contact



ERASMUS, Jacques, Etienne
8 Hillcrest
Overlane
Belper DE5 60JF
ROYAUME UNI

Date
11.01.16

Reference	Application No./Patent No. 14791882.5 - 1853 PCT/US2014036832
Applicant/Proprietor Webroot Inc.	

Notification of the data mentioned in Rule 19(3) EPC

In the above-identified patent application you are designated as inventor/co-inventor.
Pursuant to Rule 19(3) EPC the following data are notified herewith:

DATE OF FILING : 05.05.14

PRIORITY : US/03.05.13/ USP201361819470

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

DESIGNATED STATES : AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE
IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM
TR

Receiving Section





European Patent Office
80298 MUNICH
GERMANY

Questions about this communication ?
Contact Customer Services at www.epo.org/contact



LEIDESDORFF, Michael
8425 Firethorn Court
Niwt, CO 80503
ETATS-UNIS D'AMERIQUE

Date
11.01.16

Reference	Application No./Patent No. 14791882.5 - 1853 PCT/US2014036832
Applicant/Proprietor Webroot Inc.	

Notification of the data mentioned in Rule 19(3) EPC

In the above-identified patent application you are designated as inventor/co-inventor.
Pursuant to Rule 19(3) EPC the following data are notified herewith:

DATE OF FILING : 05.05.14
PRIORITY : US/03.05.13/ USP201361819470
TITLE : METHOD AND APPARATUS FOR PROVIDING FORENSIC
VISIBILITY INTO SYSTEMS AND NETWORKS
DESIGNATED STATES : AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE
IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM
TR

Receiving Section





European Patent Office
80298 MUNICH
GERMANY

Questions about this communication ?
Contact Customer Services at www.epo.org/contact



JAROSH, Joseph, A.
20540 N. Westpark Place
Deer Park, IL 60010
ETATS-UNIS D'AMERIQUE

Date
11.01.16

Reference	Application No./Patent No. 14791882.5 - 1853 PCT/US2014036832
Applicant/Proprietor Webroot Inc.	

Notification of the data mentioned in Rule 19(3) EPC

In the above-identified patent application you are designated as inventor/co-inventor.
Pursuant to Rule 19(3) EPC the following data are notified herewith:

DATE OF FILING : 05.05.14
PRIORITY : US/03.05.13/ USP201361819470
TITLE : METHOD AND APPARATUS FOR PROVIDING FORENSIC
VISIBILITY INTO SYSTEMS AND NETWORKS
DESIGNATED STATES : AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE
IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM
TR

Receiving Section





European Patent Office
80298 MUNICH
GERMANY

Questions about this communication ?
Contact Customer Services at www.epo.org/contact



BACHER, Chad, Edward
13328 W. 87th Terrace
Arvada, CO 80005
ETATS-UNIS D'AMERIQUE

Date
11.01.16

Reference	Application No./Patent No. 14791882.5 - 1853 PCT/US2014036832
Applicant/Proprietor Webroot Inc.	

Notification of the data mentioned in Rule 19(3) EPC

In the above-identified patent application you are designated as inventor/co-inventor.
Pursuant to Rule 19(3) EPC the following data are notified herewith:

DATE OF FILING : 05.05.14
PRIORITY : US/03.05.13/ USP201361819470
TITLE : METHOD AND APPARATUS FOR PROVIDING FORENSIC
VISIBILITY INTO SYSTEMS AND NETWORKS
DESIGNATED STATES : AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE
IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM
TR

Receiving Section





European Patent Office
80298 MUNICH
GERMANY

Questions about this communication ?
Contact Customer Services at www.epo.org/contact



BARNES, Paul
8 Wren Way
Mickleover
Derby DE3 0UF
ROYAUME UNI

Date
11.01.16

Reference	Application No./Patent No. 14791882.5 - 1853 PCT/US2014036832
Applicant/Proprietor Webroot Inc.	

Notification of the data mentioned in Rule 19(3) EPC

In the above-identified patent application you are designated as inventor/co-inventor.
Pursuant to Rule 19(3) EPC the following data are notified herewith:

DATE OF FILING : 05.05.14
PRIORITY : US/03.05.13/ USP201361819470
TITLE : METHOD AND APPARATUS FOR PROVIDING FORENSIC
VISIBILITY INTO SYSTEMS AND NETWORKS
DESIGNATED STATES : AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE
IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM
TR

Receiving Section





European Patent Office
80298 MUNICH
GERMANY

Questions about this communication ?
Contact Customer Services at www.epo.org/contact



GIULIANI, Marco
Via Santa Elisabetta 21C
I-06083 Bastia Umbra (PG)
ITALIE

Date
11.01.16

Reference	Application No./Patent No. 14791882.5 - 1853 PCT/US2014036832
Applicant/Proprietor Webroot Inc.	

Notification of the data mentioned in Rule 19(3) EPC

In the above-identified patent application you are designated as inventor/co-inventor.
Pursuant to Rule 19(3) EPC the following data are notified herewith:

DATE OF FILING : 05.05.14
PRIORITY : US/03.05.13/ USP201361819470
TITLE : METHOD AND APPARATUS FOR PROVIDING FORENSIC
VISIBILITY INTO SYSTEMS AND NETWORKS
DESIGNATED STATES : AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE
IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM
TR

Receiving Section





European Patent Office
80298 MUNICH
GERMANY

Questions about this communication ?
Contact Customer Services at www.epo.org/contact



WILLIAMS, Christopher, John
28 William Brown Square
Chesterfield
Derbyshire S40 2FX
ROYAUME UNI

Date
11.01.16

Reference	Application No./Patent No. 14791882.5 - 1853 PCT/US2014036832
Applicant/Proprietor Webroot Inc.	

Notification of the data mentioned in Rule 19(3) EPC

In the above-identified patent application you are designated as inventor/co-inventor.
Pursuant to Rule 19(3) EPC the following data are notified herewith:

DATE OF FILING : 05.05.14
PRIORITY : US/03.05.13/ USP201361819470
TITLE : METHOD AND APPARATUS FOR PROVIDING FORENSIC
VISIBILITY INTO SYSTEMS AND NETWORKS
DESIGNATED STATES : AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE
IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM
TR

Receiving Section





Acknowledgement of receipt

We hereby acknowledge receipt of the form for entry into the European phase (EPO as designated or elected Office) as follows:

Submission number	4006608	
PCT application number	PCT/US2014/036832	
EP application number	14791882.5	
Date of receipt	22 December 2015	
Receiving Office	European Patent Office, The Hague	
Your reference	EP103926EHjet	
Applicant		
Country		
Documents submitted	package-data.xml application-body.xml AMSPECEPO-1.pdf\EP103926_claims.pdf (6 p.)	ep-euro-pct.xml epf1200.pdf (5 p.)
Submitted by	CN=Michael Heise 38571	
Method of submission	Online	
Date and time receipt generated	22 December 2015, 16:54 (CET)	
Message Digest	9E:17:C0:AB:C8:46:75:75:33:15:DE:CD:3B:72:AA:CF:F5:DF:A3:B7	

Correction by the EPO of errors in debit instructions filed by eOLF

Errors in debit instructions filed by eOLF that are caused by the editing of Form 1038E entries or the continued use of outdated software (all forms) may be corrected automatically by the EPO, leaving the payment date unchanged (see decision T 152/82,

OJ EPO 1984, 301 and point 6.3 ff ADA, Supplement to OJ EPO 10/2007).

/European Patent Office/

NEW CLAIMS

1. A method comprising:

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

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

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

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

transmitting the assembled event line.
2. The method of claim 1, wherein the information associated with the one or more of the first object and the originating object is obtained from a community database; and
- wherein the event line is transmitted to an end recipient.
3. The method of claim 1 or 2, further comprising:

obtaining an event priority based on one or more of the generated context and the global perspective for the at least one event, wherein the event line further includes the event priority for the at least one event.
4. The method of any one of claims 1 to 3, 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; and/or
- further comprising:

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

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

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

5. The method of claim 4, 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; and/or

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.

6. A computer readable storage medium comprising processor executable instructions operable to perform the method of any one of claims 1 to 5.

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

a device including:

a communication interface;

a processor;

data storage; and

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

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

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

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

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

transmit the assembled event line utilizing the communication interface.

8. The system of claim 7, wherein the at least one of the one or more events is executed by the processor.
9. The system of claim 7 or 8, 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.
10. The system of any one of claims 7 to 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.
11. The system of any one of claims 7 to 10, wherein the sensor agent is one or more of:

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; or

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; or

further operable to:

cache the one or more events, and

asynchronously consolidate and normalize the one or more events.

12. The system of claim 10, 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.
13. 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.

14. The system of claim 13, further comprising a global perspective information server including:

a processor;

a communication interface;

data storage; and

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

receive the event line from the device;

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

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

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

15. The system of claim 13 or 14, 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; and/or

further comprising a bridge including:

a processor;

a communication interface; and

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

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

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

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

obtain a second global perspective for the another event;

provide the first global perspective to the device; and

provide the second global perspective to the another device.



Entry into the European phase (EPO as designated or elected Office)

To the European Patent Office

European application number	
PCT application number	PCT/US2014/036832
PCT publication number	WO2014179805
Applicant's or representative's reference	EP103926EHjet
International Filing Date	05.05.2014
International Searching Authority (ISA)	US
International Preliminary Examining Authority (IPEA)	not applicable
1. Applicant	
Indications concerning the applicant(s) are contained in the international publication or were recorded by the International Bureau after the international publication.	☒
Changes which have not yet been recorded by the International Bureau are set out here:	☐
2. Representative	
Representative 1	
This is the representative who will be listed in the European Patent Register and to whom notifications will be sent.	
Name:	Grünecker Patent- und Rechtsanwälte PartG mbB
Association No.:	72
Address of place of business:	Leopoldstrasse 4 80802 München, Germany
Telephone:	+49 89 21 23 50
Fax:	+49 89 22 02 87
3. Authorisation	
Representative 1	
An individual authorisation is attached.	☐
A general authorisation has been registered under No:	☐
A general authorisation has been filed, but not yet registered.	☐
The authorisation filed with the EPO as PCT receiving Office expressly includes the European phase.	☐
4. Request for examination	
Examination of the application under Art. 94 EPC is hereby requested. The examination fee is being (has been, will be) paid.	☒
Request for examination in an admissible non-EPO language:	☐
The applicant waives his right to be asked under Rule 70(2) EPC whether he wishes to proceed further with the application.	☐
The/Each applicant hereby declares that he is an entity or a natural person under Rule 6(4) EPC.	☐
5. Copies	
Additional copies of the documents cited in the supplementary European search report are requested.	☐
Number of additional sets of copies	
6. Documents intended for proceedings before the EPO	
Number of claims on entry into the European phase:	15
6.1 Proceedings before the EPO as designated Office (PCT I) are to be based on the following documents:	
the application documents published by the International Bureau (with all claims, description and drawings), where applicable with amended claims under Art. 19	☐

EP103926EHjet

unless replaced by the amendments attached.

Where necessary, clarifications should be attached as 'Other documents'

6.2 Proceedings before the EPO as elected Office (PCT II) are to be based on the following documents:

the documents on which the international preliminary examination report is based, including any annexes

unless replaced by the amendments attached.

Where necessary, clarifications should be attached as 'Other documents'

If the EPO as International Preliminary Examining Authority has been supplied with test reports, these may be used as the basis of proceedings before the EPO.

6.3 A copy of the results of the search carried out by the authority with which the previous application(s) whose priority is claimed was (were) filed is attached (R. 141(1) EPC).

6.4 The applicant waives his right to the communication under Rules 161(1) or (2) and 162 EPC.

7. Translations

Translations in one of the official languages of the EPO (English, French, German) are attached as crossed below:

* In proceedings before the EPO as designated or elected Office (PCT I + II):

Translation of the international application (description, claims, any text in the drawings) as originally filed, of the abstract as published and of any indication under Rule 13bis.3 and 13bis.4 PCT regarding biological material

Translation of the priority application(s) (to be filed only at the EPO's request, Rule 53(3) EPC)

It is hereby declared that the international application as originally filed is a complete translation of the previous application (Rule 53(3) EPC)

** In addition, in proceedings before the EPO as designated Office (PCT I):*

Translation of amended claims and any statement under Art. 19 PCT, if the claims as amended are to form the basis for the proceedings before the EPO (see Section 6).

** In addition, in proceedings before the EPO as elected Office (PCT II):*

Translation of annexes to the international preliminary examination report

8. Biological material

The invention uses and/or relates to biological material deposited under Rule 31 EPC.

The particulars referred to in Rule 31(1)(c) EPC (if not yet known, the depositary institution and the identification reference(s) [number, symbols, etc.] of the depositor) are given in the international publication or in the translation submitted in Section 7 on:

page(s) / line(s)

The receipt(s) of deposit issued by the depository institution is (are) enclosed.

will be filed later.

Waiver of the right to an undertaking from the requester pursuant to Rule 33(2) EPC attached.

9. Nucleotide and amino acid sequences

The international application discloses nucleotide and/or amino acid sequences.

9.1 The sequence listing was filed under Rule 5.2(a) PCT, or furnished to the EPO as ISA under Rule 13ter.1(a) PCT, or is otherwise available to the EPO, in computer-readable format in accordance with WIPO ST.25.

9.2

The sequence listing is attached in computer-readable format in accordance with WIPO Standard ST.25

The sequence listing is attached in PDF format.

The sequence listing does not include matter which goes beyond the content of the application as filed.

EP103926EHjet

10. Designation of contracting states All the contracting states party to the EPC at the time of filing of the international patent application and designated in the international application are deemed to be designated (see Article 79(1) EPC).		☒		
11. Extension/Validation This application is deemed to be a request to extend the effects of the European patent application and the European patent granted in respect of it to all non-contracting states to the EPC designated in the international application with which extension or validation agreements were in force on the date on which the application was filed. However, the request is deemed withdrawn if the extension fee or the validation fee, whichever is applicable, is not paid within the prescribed time limit. 11.1 It is intended to pay the extension fee(s) for the following state(s): 11.2 It is intended to pay the validation fee(s) for the following state(s): Note: Under the automatic debiting procedure, extension and/or validation fees will be debited only for states indicated here unless the EPO is instructed otherwise before expiry of the period for payment.		☐		
12. List of enclosed documents				
	Description of document	Original file name	Assigned file name	
1	Combined Amendments	EP103926_claims.pdf	AMSPECEPO-1.pdf	
13. Mode of payment: Debit from deposit account Currency The European Patent Office is hereby authorised, to debit from the deposit account with the EPO any fees and costs indicated on the fees page. Deposit account number Account holder		☒ EUR 28000437 Grünecker Patent- und Rechtsanwälte PartG mbB		
14. Any refunds should be made to the following EPO deposit account: Number and account holder		☒ Grünecker Patent- und Rechtsanwälte PartG mbB, 28000437		
15. Fees				
		Factor/reducti on applied	Fee schedule	Amount to be paid
15-1	002 Fee for a European search - Applications filed on/after 01.07.2005	-190	1 285.00	1 095.00
15-2	005e Designation fee - For all contracting States designated for applications filed on/after 01.04.2009	1	580.00	580.00
15-3	006 Examination fee - For applications filed on/after 01.07.2005	1	1 620.00	1 620.00
15-4	015 Claims fee - For the 16th to the 50th claim	0	235.00	0.00
15-5	15e Claims fee - For the 51st and each subsequent claim	0	580.00	0.00
15-6	020 Filing fee - entry EP phase - online	1	120.00	120.00
15-7	055 Additional copy	0	40.00	0.00
15-8	122 Fee for further processing (non fee related cases)	1	250.00	250.00
15-9	123 Fee for further processing (late payment of a fee - 50%)	1	1 865.00	1 865.00
15-10	520 Additional filing fee for the 36th and each subsequent page - entry into EP phase	21	15.00	315.00
	Total:		EUR	5 845.00
16. Annotations				
17. Signature(s) of applicant(s) or representative				

EP103926EHjet

Place: Munich
Date: 22 December 2015
Signed by: Michael Heise 38571
Association: Grünecker Patent- und Rechtsanwälte PartG
mbB
Representative name: Michael Heise
Capacity: (Representative)

Table for section 6 of Form 1200.3

In accordance with the Notice from the European Patent Office dated 26 January 2009 concerning the 2009 fee structure (OJ EPO 2009, 118, and Guidelines for Examination in the EPO, April 2009, A-III, 13.2), the amount of the additional fee (Art. 2, item 1a, Rules relating to Fees) for the pages of this European patent application is calculated as follows:

Documents intended for proceedings before the EPO (R. 159 (1) (b) EPC) and for calculating the additional fee (Art. 2, item 1a, RFees):

	Page(s) from ... to ...	Number of pages
Description: International application as published	1-34	34
Claims: Amendments filed on entry into European phase	1-6	6
Drawings: International application as published	1-15	15
Abstract: Default count: one page		1
Total number of pages		56
Fee-exempt pages (Art. 2, item 1a, RFees)		-35
Number of pages to be paid for		21
		(x 15 EUR per page)
Total amount payable	EUR	315

EP103926EHjet

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

(Chapter I of the Patent Cooperation Treaty)

(PCT Rule 44bis)

Applicant's or agent's file reference 6890-103-PCT	FOR FURTHER ACTION		See item 4 below
International application No. PCT/US2014/036832	International filing date (<i>day/month/year</i>) 05 May 2014 (05.05.2014)	Priority date (<i>day/month/year</i>) 03 May 2013 (03.05.2013)	
International Patent Classification (8th edition unless older edition indicated) See relevant information in Form PCT/ISA/237			
Applicant WEBROOT INC.			

1. This international preliminary report on patentability (Chapter I) is issued by the International Bureau on behalf of the International Searching Authority under Rule 44 bis.1(a).

2. This REPORT consists of a total of 8 sheets, including this cover sheet.

In the attached sheets, any reference to the written opinion of the International Searching Authority should be read as a reference to the international preliminary report on patentability (Chapter I) instead.

3. This report contains indications relating to the following items:

- | | | |
|-------------------------------------|--------------|---|
| ☒ | Box No. I | Basis of the report |
| ☐ | Box No. II | Priority |
| ☐ | Box No. III | Non-establishment of opinion with regard to novelty, inventive step and industrial applicability |
| ☐ | Box No. IV | Lack of unity of invention |
| ☒ | Box No. V | Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement |
| ☐ | Box No. VI | Certain documents cited |
| ☐ | Box No. VII | Certain defects in the international application |
| ☐ | Box No. VIII | Certain observations on the international application |

4. The International Bureau will communicate this report to designated Offices in accordance with Rules 44bis.3(c) and 93bis.1 but not, except where the applicant makes an express request under Article 23(2), before the expiration of 30 months from the priority date (Rule 44bis .2).

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No. +41 22 338 82 70		Date of issuance of this report 03 November 2015 (03.11.2015) Authorized officer Agnès Wittmann-Regis e-mail: pt06.pct@wipo.int
---	--	---

Form PCT/IB/373 (January 2004)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To: BRENT R. LINDON
SHERIDAN ROSS P.C.
1560 BROADWAY
SUITE 1200
DENVER, CO 80202

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43bis.1)

Date of mailing
(day/month/year)

29 SEP 2014

Applicant's or agent's file reference
6890-103-PCT

FOR FURTHER ACTION

See paragraph 2 below

International application No.

PCT/US2014/036832

International filing date (day/month/year)

05 May 2014

Priority date (day/month/year)

03 May 2013

International Patent Classification (IPC) or both national classification and IPC

IPC(8) - G06F21/00 (2014.01)

CPC - H04L63/14 (2014.02)

Applicant WEBROOT INC.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1 bis(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA/US
Mail Stop PCT, Attn: ISA/US
Commissioner for Patents
P.O. Box 1450, Alexandria, Virginia 22313-1450
Facsimile No. 571-273-3201

Date of completion of this opinion

09 September 2014

Authorized officer:

Blaine R. Copenheaver

PCT Helpdesk: 571-272-4300
PCT OSP: 571-272-7774

Form PCT/ISA/237 (cover sheet) (July 2011)

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.

PCT/US2014/036832

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:
 - ☒ the international application in the language in which it was filed.
 - ☐ a translation of the international application into _____ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).
2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43bis.1(a))
3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing filed or furnished:
 - a. (means)
 - ☐ on paper
 - ☐ in electronic form
 - b. (time)
 - ☐ in the international application as filed
 - ☐ together with the international application in electronic form
 - ☐ subsequently to this Authority for the purposes of search
4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.
5. Additional comments:

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.

PCT/US2014/036832

Box No. V	Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement			
1. Statement				
Novelty (N)	Claims	5-7, 14-16, 19-20	YES	
	Claims	1-4, 8-13, 17-18	NO	
Inventive step (IS)	Claims	None	YES	
	Claims	1-20	NO	
Industrial applicability (IA)	Claims	1-20	YES	
	Claims	None	NO	
2. Citations and explanations:				
Claims 1-4, 8-13 and 17-18 lack novelty under PCT Article 33(2) as being anticipated by Morris et al. (hereinafter Morris). Regarding claim 1, Morris teaches a method (abstract) comprising: gathering one or more events defining an action of a first object acting on a target (para [0056] discloses an agent program running on a remote computer searches a local database for information related to events, where, as further disclosed in para [0056], events define the actions or behaviors of an object acting upon another object. The event includes the key of the object performing the act [claimed first object] and the identity of another object which the act is being performed on [claimed target]); generating a contextual state for at least one of the one or more events by correlating the at least one event to an originating object (para [0055], discloses generating metadata [claimed contextual state], where, as further disclosed in para [0058], the metadata includes Genesisactor information which includes the parent of the object being performed [claimed originating object]). For example in the case of a software installation, this would be the key of the object that the user or system first executed and that initiated the software installation process, e.g. Setup.exe), the contextual state including an indication of the originating object of the first object (para [0058], the metadata includes Genesisactor information which includes the parent of the object being performed [claimed originating object of the first object]) and an indication of at least one of a device on which the first object is executed and a user associated with the first object (para [0119] discloses metadata may include operating system of the remote computer that encountered the object [claimed indication of a device] and author of the object [claimed user associated with the first object]); obtaining a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object (para [0125], a collective view of the object, i.e. its meta data and behaviors, across all agents that have seen it, provides an informed view [thus, a collective view [claimed global perspective] of the object is established by allowing agents to analyze and share obtained metadata relating to objects). Further, as disclosed in para [0056] and [0058], the metadata information may include information of the object performing the act [claimed first object], the event type and the parent object [claimed originating object]), the information including at least one of age (para [0134], objects having a specific determination, location, popularity, age or any other criteria known by or derived by the database), popularity (para [0134]), a determination as to whether the first object is malware (para [0015], determine whether or not the object is malware), a determination as to whether the originating object is malware (determine whether or not the object is malware. Also see para [0058]); and Internet Protocol (IP) Address or Uniform Resource Locator (URL) information (para [0056], the IP address or URL); assembling an event line including details associated with the at least one event, the details including information uniquely identifying each of the first object (para [0046], the details of an object that are passed to the base computer may be in the form of a signature or "key" that uniquely identifies the object), the action of the first object (para [0055]-[0056], metadata details captured and sent include events, which define the actions or behaviors of an object), the target (para [0056], victim), and the originating object (para [0058], parent object); and transmitting the assembled event line (para [0046], The details of an object that are passed [claimed transmitting] to the base computer. Further, as disclosed in para [0055], metadata details are passed [claimed transmitting] to the base computer.). Regarding claim 2, Morris teaches wherein the information associated with the one or more of the first object and the originating object is obtained from a community database (para [0061], community database of metadata information); and wherein the event line is transmitted to an end recipient (para [0125], collected metadata can be retrieved by a human [claimed end recipient]). Regarding claim 3, Morris teaches obtaining an event priority based on one or more of the generated context and the global perspective for the at least one event (para [0061] discloses generating rules using metadata [claimed context] received from remote computers, where as further disclosed in para [0056], the metadata includes event information. Further, as disclosed in para [0134], rules may be prioritized and applied against objects with specific metadata [the prioritized rules are based on specific metadata [claimed context], which include event information, thus a specific event an associated priority]), wherein the event line further includes the event priority for the at least one event (para [0134] discloses associating a prioritized rule with metadata information, where, as further disclosed in para [0056], the metadata information includes event information. Further, as disclosed in para [0061], the database creates stores and transmits details of the rules [claimed event line] to be applied by the remote computers [thus, the database maintains details [claimed event line] of the prioritized rules associated with the monitored events]). Regarding claim 4, Morris teaches wherein the at least one event includes information uniquely identifying the object performing the action (para [0056], the event includes information of the object performing the act), information uniquely identifying the action being performed (para [0056], the event includes information of the act being performed), and information uniquely identifying the target upon which the act is being performed (para [0056], the event includes the object or identity of another entity upon which the act is being performed). Regarding claim 8, Morris teaches a computer readable storage medium comprising processor executable 20 instructions operable to perform the method of claim 1 (para [0156]-[0157]).				

Form PCT/ISA/237 (Box No. V) (July 2011)

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.

PCT/US2014/036832

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of:

Regarding claims 9 and 17, Morris teaches a system for providing forensic visibility into a system (para [0142], forensic data handling), comprising: a device including: a communication interface; a processor; data storage; and a sensor agent stored on the data storage that is executable by the processor (para [0018], agent program [claimed sensor agent] installed on a remote computer [claimed device]). Also see para [0156]), wherein the sensor agent is operable to: (para [0056] discloses an agent program running on a remote computer searches a local database for information related to events, where, as further disclosed in para [0056], events define the actions or behaviors of an object acting upon another object. The event includes the key of the object performing the act [claimed first object] and the identity of another object which the act is being performed on [claimed target]); generating a contextual state for at least one of the one or more events by correlating the at least one event to an originating object (para [0055], discloses generating metadata [claimed contextual state], where, as further disclosed in para [0058], the metadata includes Genesisactor information which includes the parent of the object being performed [claimed originating object]. For example in the case of a software installation, this would be the key of the object that the user or system first executed and that initiated the software installation process, e.g. Setup.exe, the contextual state including an indication of the originating object of the first object (para [0058], the metadata includes Genesisactor information which includes the parent of the object being performed [claimed originating object of the first object] and an indication of at least one of a device on which the first object is executed and a user associated with the first object (para [0119] discloses metadata may include operating system of the remote computer that encountered the object [claimed indication of a device] and author of the object [claimed user associated with the first object]); obtaining a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object (para [0125], a collective view of the object, i.e. its meta data and behaviors, across all agents that have seen it, provides an informed view [thus, a collective view [claimed global perspective] of the object is established by allowing agents to analyze and share obtained metadata relating to objects). Further, as disclosed in para [0056] and [0058], the metadata information may include information of the object performing the act [claimed first object], the event type and the parent object [claimed originating object]), the information including at least one of age (para [0134], objects having a specific determination, location, popularity, age or any other criteria known by or derived by the database), popularity (para [0134]), a determination as to whether the first object is malware (para [0015], determine whether or not the object is malware), a determination as to whether the originating object is malware (determine whether or not the object is malware. Also see para [0058]); and Internet Protocol (IP) Address or Uniform Resource Locator (URL) information (para [0056], the IP address or URL); assembling an event line including details associated with the at least one event, the details including information uniquely identifying each of the first object (para [0046], the details of an object that are passed to the base computer may be in the form of a signature or "key" that uniquely identifies the object), the action of the first object (para [0055]-0056), metadata details captured and sent include events, which define the actions or behaviors of an object), the target (para [0056], victim), and the originating object (para [0058], parent object); and transmitting the assembled event line utilizing the communication interface (para [0046], The details of an object that are passed [claimed transmitting] to the base computer. Further, as disclosed in para [0055], metadata details are passed [claimed transmitting] to the base computer, where, as further disclosed in para [0061], the metadata information is derived from the remote computers [thus, the remote computers, which includes the agent program, will send the metadata information through an associated interface]. Also see para [0014]).

Regarding claim 10, Morris teaches wherein the at least one of the one or more events is executed by the processor (para [0156]).

Regarding claim 11, Morris teaches a global perspective information server (para [0073], ENZO central servers that aggregate all of the collected data); and an end recipient device (para [0125], human access collected data), wherein the information associated with the one or more of the first object and the originating object is obtained from the global perspective information server (para [0091] discloses the ENZO server propagates metadata information to remote computers, where, as further disclosed in para [0056] and [0058], the metadata information may include information of the object performing the act [claimed first object] and the parent object [claimed originating object]) and the sensor agent transmits the event line to the end recipient (para [0055], metadata details are passed [claimed transmitting] to the base computer, where, as further disclosed in para [0061], the metadata information is derived from the remote computers [thus, the remote computers, which includes the agent program, will send the metadata information through an associated interface]. Also see para [0014]).

Regarding claim 12, Morris teaches wherein the sensor agent is further operable to: cache the one or more events (para [0035], a local agent [claimed sensor agent] of a remote computer searches a local database stored at the remote computer. Further, as disclosed in para [0039], the local database copies the signature information from a community database for retrieval [thus, the information is cached locally for faster retrieval]); and asynchronously consolidate and normalize the one or more events (para [0093], the agent program on the remote computer coordinates with the ENZO server to update metadata information about which objects have been seen by the community so as not to store duplicated metadata, where, as further disclosed in para [0056], the metadata includes event information. Further, as disclosed in para [0093], this process is initiated when the remote computers and the associated agents receive a data packet [thus, each remote computer will initiate the coordination with the ENZO server dynamically and not in a synchronized operation]).

Regarding claim 13, Morris teaches wherein the at least one event includes information uniquely identifying the object performing the action (para [0056], the event includes information of the object performing the act), information uniquely identifying the action being performed (para [0056], the event includes information of the act being performed), and information uniquely identifying the target upon which the act is being performed (para [0056], the event includes the object or identity of another entity upon which the act is being performed).

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.
PCT/US2014/036832

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of:

Regarding claim 18, Morris teaches a global perspective information server (para [0073], ENZO central servers that aggregate all of the collected data) including: a processor ([0156]); a communication interface (para [0093] discloses the ENZO server communicates with remote computers [thus, the server will have an associated interface]; data storage (para [0093], ENZO server stores metadata information. Also see para [0073]); and a global perspective module, wherein the global perspective module is operable to: receive the event line from the device (para [0073] discloses aggregate all of the information received from all remote computers [thus, the server will have a global perspective of all metadata information]. Also see para [0074]-[0076] and [0093]); obtain a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object (para [0093] discloses the ENZO server stores all metadata information, where, as further disclosed in para [0056] and [0058], the metadata information may include information of the object performing the act [claimed first object] and the parent object [claimed originating object]), the information including at least one of age (para [0134], objects having a specific determination, location, popularity, age or any other criteria known by or derived by the database), popularity (para [0134]), a determination as to whether the first object is malware (para [0015], determine whether or not the object is malware), a determination as to whether the originating object is malware (determine whether or not the object is malware. Also see para [0058]); and Internet Protocol (IP) Address or Uniform Resource Locator (URL) information (para [0056], the IP address or URL); assemble a second event line including details associated with the at least one event (para [0093] discloses the ENZO server maintains a master list [claimed second event line] of all metadata information and propagates the list to all remote computers), the details including information uniquely identifying each of the first object (para [0056], metadata information includes events related to objects performing the act), the action of the first object (para [0056] discloses metadata information includes the act being performed), the target (para [0056] discloses metadata information includes the victim), and the originating object (para [0058], metadata information includes parent object); and transmit the assembled second event line utilizing the communication interface to an end recipient (para [0093] discloses the ENZO server maintains a master list [claimed second event line] of all metadata information and propagates the list to all remote computers).

Claims 7, 16 and 19 lack an inventive step under PCT Article 33(3) as being obvious over Morris.

Regarding claim 7, Morris teaches heuristically displaying information identifying the first object performing the action (para [0125] discloses displaying the collected information regarding the monitored objects, where, as further disclosed in para [0061], the collected information in the database include rules and heuristics), information identifying the action being performed (para [0056]), information identifying the target upon which the act is being performed (para [0056]), and the global perspective according to one or more of a location associated with the first object (para [0125] discloses obtaining a collective view of an object including its metadata and behaviors, where, as further disclosed in para [0057], the metadata includes location information. Also see para [0119]); at least one characteristic of an outbound connection associated with the first object (para [0056], a network entity with which an object is communicating); a executable file (para [0111], The data can also be measured against their filenames, and file types (e.g. .exe) [claimed executable file]. Also see para [0058]); an age of the first object (para [0044] discloses monitoring a process [claimed object] for a period of n days [claimed age] to determine whether the process is safe. Also see para [0132]); and connections associated with the first object (para [0056], a network entity with which an object is communicating).

Morris does not teach identifying dropped files and a number of concurrent connections. However, configuring management of data and data connections has been a practice well known in the art and the specifics (identifying dropped files and a number of concurrent connections) would have been a matter of design choice. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate identifying dropped files and a number of concurrent connections in the invention of Morris. The motivation do so would have been to enhance the detection of security attacks by collecting and displaying security related information (Morris, para [0125]).

Regarding claim 16, Morris teaches heuristically displaying information identifying the first object performing the action (para [0125] discloses displaying the collected information regarding the monitored objects, where, as further disclosed in para [0061], the collected information in the database include rules and heuristics), information identifying the action being performed (para [0056]), information identifying the target upon which the act is being performed (para [0056]), and the global perspective according to one or more of a location associated with the first object (para [0125] discloses obtaining a collective view of an object including its metadata and behaviors, where, as further disclosed in para [0057], the metadata includes location information. Also see para [0119]); at least one characteristic of an outbound connection associated with the first object (para [0056], a network entity with which an object is communicating); a executable file (para [0111], The data can also be measured against their filenames, and file types (e.g. .exe) [claimed executable file]. Also see para [0058]); an age of the first object (para [0044] discloses monitoring a process [claimed object] for a period of n days [claimed age] to determine whether the process is safe. Also see para [0132]); and connections associated with the first object (para [0056], a network entity with which an object is communicating).

Morris does not teach identifying dropped files and a number of concurrent connections. However, configuring management of data and data connections has been a practice well known in the art and the specifics (identifying dropped files and a number of concurrent connections) would have been a matter of design choice. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate identifying dropped files and a number of concurrent connections in the invention of Morris. The motivation do so would have been to enhance the detection of security attacks by collecting and displaying security related information (Morris, para [0125]).

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.
PCT/US2014/036832

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of:

Regarding claim 19, Morris teaches wherein the end recipient heuristically displays information identifying the first object performing the action (para [0125] discloses displaying the collected information regarding the monitored objects, where, as further disclosed in para [0061], the collected information in the database include rules and heuristics), information identifying the action being performed (para [0056]), information identifying the target upon which the act is being performed (para [0056]), and the global perspective according to one or more of a location associated with the first object (para [0125] discloses obtaining a collective view of an object including its metadata and behaviors, where, as further disclosed in para [0057], the metadata includes location information. Also see para [0119]); at least one characteristic of an outbound connection associated with the first object (para [0056], a network entity with which an object is communicating); a executable file (para [0111], The data can also be measured against their filenames, and file types (e.g. .exe) [claimed executable file]. Also see para [0058]); an age of the first object (para [0044] discloses monitoring a process [claimed object] for a period of n days [claimed age] to determine whether the process is safe. Also see para [0132]); and connections associated with the first object (para [0056], a network entity with which an object is communicating).

Morris does not teach identifying dropped files and a number of concurrent connections. However, configuring management of data and data connections has been a practice well known in the art and the specifics (identifying dropped files and a number of concurrent connections) would have been a matter of design choice. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate identifying dropped files and a number of concurrent connections in the invention of Morris. The motivation do so would have been to enhance the detection of security attacks by collecting and displaying security related information (Morris, para [0125]).

Claims 5-6 and 14-15 lack an inventive step under PCT Article 33(3) as being obvious over Morris in view of Crosby et al (hereinafter Crosby).

Regarding claim 5, Morris teaches determining whether [information] for the at least one event has been cached (para [0035], search a local database stored at the remote computer to search for a signature or key representing that particular process, its related objects and/or the event. Further, as disclosed in para [0039], the local database copies the signature information from a community database for retrieval [thus, the information is cached locally for faster retrieval]); when the [information] for the at least one event has been cached, obtaining [information] for the at least one event based on the cached information (para [0035], If the local signature is present, it will indicate either that the process is considered to be safe or will indicate that that process is considered unsafe [claimed obtaining information based on the stored information]); and when the [information] for the at least one event has not been cached, obtaining [information] for the at least one event from a community database (para [0039], when a local signature is not found, a community database is searched and used to retrieve the required signature information which is sent to the local computer).

Morris does not teach caching a global perspective. However, Crosby, in analogous art, teaches monitoring security attacks (abstract). Crosby further teaches caching a global perspective (para [0042] discloses a locally storing global beliefs [claimed global perspective] regarding the security state of the system. Also see para [0023] and [0025]). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Crosby to incorporate caching a global perspective in the invention of Morris in order to enhance detection of security attacks (Crosby, para [0042]).

Regarding claim 6, Morris teaches obtaining [information] for the at least one event from a community database (para [0039]). Morris does not teach determining whether the cached global perspective for the at least one event has expired; and when the global perspective for the at least one event has expired, obtaining a global perspective for the at least one event from a database. However Crosby, in analogous art, teaches determining whether the cached global perspective for the at least one event has expired (para [0043] discloses whether global beliefs are older than a maximum age value [claimed expired]); and when the global perspective for the at least one event has expired (para [0043], determine whether global belief has exceeded maximum age. Also see para [0023]). Furthermore, configuring management of data has been a practice well known in the art and the specifics (obtaining a global perspective from a database when the global perspective has expired) would have been a matter of design choice. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Crosby to incorporate retrieval of information from a database when the information has expired in the invention of Morris in order to enhance the detection of new security attacks (Crosby, para [0043]).

Regarding claim 14, Morris teaches determining whether [information] for the at least one event has been cached (para [0035], search a local database stored at the remote computer to search for a signature or key representing that particular process, its related objects and/or the event. Further, as disclosed in para [0039], the local database copies the signature information from a community database for retrieval [thus, the information is cached locally for faster retrieval]); when the [information] for the at least one event has been cached, obtaining [information] for the at least one event based on the cached information (para [0035], If the local signature is present, it will indicate either that the process is considered to be safe or will indicate that that process is considered unsafe [claimed obtaining information based on the stored information]); and when the [information] for the at least one event has not been cached, obtaining [information] for the at least one event from a community database (para [0039], when a local signature is not found, a community database is searched and used to retrieve the required signature information which is sent to the local computer).

Morris does not teach caching a global perspective. However, Crosby, in analogous art, teaches monitoring security attacks (abstract). Crosby further teaches caching a global perspective (para [0042] discloses a locally storing global beliefs [claimed global perspective] regarding the security state of the system. Also see para [0023] and [0025]). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Crosby to incorporate caching a global perspective in the invention of Morris in order to enhance detection of security attacks (Crosby, para [0042]).

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.
PCT/US2014/036832

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of:

Regarding claim 15, Morris teaches obtaining [information] for the at least one event from a community database (para [0039]). Morris does not teach determining whether the cached global perspective for the at least one event has expired; and when the global perspective for the at least one event has expired, obtaining a global perspective for the at least one event from a database. However Crosby, in analogous art, teaches determining whether the cached global perspective for the at least one event has expired (para [0043] discloses whether global beliefs are older than a maximum age value [claimed expired]); and when the global perspective for the at least one event has expired (para [0043], determine whether global belief has exceeded maximum age. Also see para [0023]). Furthermore, configuring management of data has been a practice well known in the art and the specifics (obtaining a global perspective from a database when the global perspective has expired) would have been a matter of design choice. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Crosby to incorporate retrieval of information from a database when the information has expired in the invention of Morris in order to enhance the detection of new security attacks (Crosby, para [0043]).

Claims 20 lack an inventive step under PCT Article 33(3) as being obvious over Morris in view of Fanton et al. (hereinafter Fanton)

Regarding claim 20, Morris teaches a bridge (para [0035], local database) including: a processor (para [0156]); a communication interface (para [0065], the agent program communicates with the local database [thus, the local database will have an associated interface to communicate]; and a cached event store (para [0065], local database holds a local copy [claimed cache] of signatures relating to the objects found on the remote computer), wherein the cached event store is operable to: receive a first request for [information] for the at least one event (para [0035], the local database is searched for signature or key representing a process, its related objects and/or event); receive a second request for a [information] for another event (para [0035] discloses searching a local database to determine whether a monitored object is safe or unsafe [thus, for each new monitored object received at the remote computer, a local database will be searched for associated information regarding the object and its related events]), obtain a first [information] for the at least one event by obtaining information associated with one or more of the first object and the originating object (para [0034]-[0035] discloses searching a local database for metadata information, where, as further disclosed in para [0056] and [0058], the metadata information may include information of the object performing the act [claimed first object] and the parent object [claimed originating object]), the information including at least one of para [0134], objects having a specific determination, location, popularity, age or any other criteria known by or derived by the database), popularity (para [0134]), a determination as to whether the first object is malware (para [0015], determine whether or not the object is malware), a determination as to whether the originating object is malware (determine whether or not the object is malware. Also see para [0058]); and Internet Protocol (IP) Address or Uniform Resource Locator (URL) information (para [0056], the IP address or URL); obtain a second [information] for the another event (para [0035] discloses searching a local database to determine whether a monitored object is safe or unsafe [thus, for each new monitored object received at the remote computer, a local database will be searched for associated information regarding the object and its related events]); provide the first [information] to the device (para [0035]);

Morris does not teach receive a request for global perspective, a second request for a global perspective from another device, provide the first global perspective to the first device and the second global perspective to the another device. However, Fanton, in analogous art, teaches protecting a computer system from attack (para [0022]). Fanton further teaches receive a request for global perspective, a second request for a global perspective from another device, provide the first global perspective to the first device and the second global perspective to the another device (para [0009] discloses generating and searching [claimed request] a global white list [claimed global perspective] to determine if a program is safe to run, where, as further disclosed in para [0039], the global white list may be maintained in a server for an enterprise network to provide a group wide policy [thus, a first and second end user of the enterprise will search a global white list stored on the server to receive a determination on the end user device to run the program]). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Fanton to incorporate send global perspective information to a first and second device in the invention of Morris in order to enhance the security of enterprise networks (Fanton, para [0039]).

Claims 1-20 meet the criteria set out in PCT Article 33(4), and thus have industrial applicability because the subject matter claimed can be made or used in industry.



European Patent Office
80298 MUNICH
GERMANY

Questions about this communication ?
Contact Customer Services at www.epo.org/contact



LINDON, Brent, R.
Sheridan Ross P.C.
1560 Broadway
Suite 1200
Denver, CO 80202
ETATS-UNIS D'AMERIQUE

Date
11.09.15

Reference	Application No./Patent No. 14791882.5 - 1853 PCT/US2014036832
Applicant/Proprietor Webroot Inc.	

Entry into the European phase before the European Patent Office

The following information describes the procedural steps required for entry into the European phase before the European Patent Office (EPO). You are advised to read it carefully because failure to take the necessary action in due time can lead to a loss of rights.

1. The above mentioned international patent application has been given the **European application No. 14791882.5**.
2. Applicants **without a residence or their principal place of business** in an EPC Contracting State may themselves initiate European processing of their international applications, provided they do so before expiry of the 31st month from the priority date.

During the European phase before the EPO as designated or elected Office, however, such applicants **must** be represented by a professional representative (Art. 133(2) and Art. 134(1) and (8) EPC).

Where, at the expiry of the time period laid down in Rule 163(5) EPC, the requirements of Article 133(2) EPC have not been complied with, the European patent application will be **refused**, pursuant to Rule 163(6) EPC.

Please note that a professional representative authorised to act before the EPO and who acted for the applicant during the international phase does not automatically become the representative for the European phase. Applicants are therefore strongly advised to appoint in good time any representative they wish to initiate the European phase for them; otherwise the EPO has to send all communications directly to the applicant.

3. Applicants **with a residence or their principal place of business** in an EPC Contracting State are not obliged to appoint for the European phase a professional representative authorised to act before the EPO. However, in view of the complexity of the procedure it is recommended that they do so.
4. Applicants and professional representatives are also strongly advised to initiate the European phase using **EPO Form 1200**. It is available free of charge from the EPO or via the EPO website at www.epo.org. Similarly, it can be or generated with the Online Filing software, obtainable free of charge from the EPO (www.epoline.org) The use of the form is not compulsory.

-
5. Applicants wishing to use an address for correspondence which is different from the address of their seat or residence are advised to indicate this address in section 1 of EPO Form 1200. When acting as designated or elected Office, the EPO will accept an address for correspondence only if no professional representative must be or is appointed (Art. 133 and 134 EPC). This address must be the applicant's own address and must be located in an EPC Contracting State. Any address for correspondence accepted for the procedure in the international phase which does not fulfil those conditions will not be accepted in the procedure before the EPO in the European phase.
6. Where the EPO acts as designated or elected Office (Art. 22(1) and (3) and 39(1) PCT), to enter the European phase before the EPO, the **following acts** must be performed by the applicant within **31 months** from the date of filing of the international application or (where applicable) the earliest priority date:
- a) Supply a translation of the international application into an EPO official language, if the International Bureau did not publish the application in such language (Art. 22(1) PCT and R. 159(1)(a) EPC);
 - b) Specify the application documents, as originally filed or as amended, on which the European grant procedure is to be based (R. 159(1)(b) EPC);
 - c) Pay the filing fee and, where applicable, the additional fee for a European patent application comprising more than 35 pages (R. 159(1)(c) EPC, Art. 2, items 1, 1a Rules relating to Fees);
 - d) Pay the search fee where a supplementary European search report has to be drawn up (R. 159(1)(e) EPC);
 - e) Pay the designation fee if the time limit laid down in Rule 39(1) EPC (i.e. six months after publication of the international search report) has expired before the 31-month period pursuant to Rule 159(1) EPC (R. 159(1)(d) EPC);
 - f) File the written request for examination and pay the examination fee if the time limit laid down in Rule 70(1) EPC has expired before the 31-month period pursuant to Rule 159(1) EPC (R. 159(1)(f) EPC);
 - g) Pay the renewal fee in respect of the third year, if the fee has fallen due (see Rule 51(1) EPC) before expiry of the 31-month period pursuant to Rule 159(1) EPC (R. 159(1)(g) EPC);
 - h) File, where applicable, the certificate of exhibition referred to in Article 55(2) and Rule 25 EPC (R. 159(1)(h) EPC);
 - i) Pay the claims fees for the sixteenth and each subsequent claim when the application documents on which the European grant procedure is to be based comprise more than fifteen claims (R. 162(1) EPC). For applications entering the European phase on or after 1 April 2009, a higher amount is payable for the 51st and each subsequent claim (Decision of the Administrative Council of 14 December 2007 amending the Rules relating to Fees, OJ EPO 2008, 10).

If either the translation of the international application or the request for examination is not filed in time, or if the filing fee, the additional fee, the search fee, the designation fee or the examination fee is not paid in due time, the application shall be deemed to be withdrawn (R. 160(1) EPC).

7. Payment of fees

An up-to-date guidance for the payment of fees, expenses and prices and a list of the euro accounts of the European Patent Organisation are published in each issue of the Official Journal of the EPO. The guidance includes inter alia a reference to the latest version of the Schedule of fees and expenses where the amounts of fees are set out.

The Schedule of fees and expenses, published as a Supplementary publication to the Official Journal of the EPO, is also available on the EPO website (www.epo.org) and can be found under www.epo.org/schedule-of-fees, which allows the viewing, downloading and searching for individual fee amounts, both current and previous.

Applicants should always check the fee amounts applying at the time of payment.

Payments can be validly made by any person. Permissible methods of payment are laid down in Article 5 Rules relating to Fees. Please note that payment cannot be made by cheque sent to the EPO.

For information on the calculation of the additional fee for applications comprising more than 35 pages, see Notice from the European Patent Office dated 26 January 2009 concerning the 2009 fee structure (OJ EPO 2009, 118), Notice supplementing the notice from the European Patent Office dated 26 January 2009 concerning the 2009 fee structure (OJ EPO 2009, 338) and Guidelines for Examination in the EPO, April 2010, A-III, 13.2.

For an overview of search and examination fees, see Notice from the European Patent Office dated 10 February 2014 (OJ EPO 2014, A31). Fee information is also published on the EPO website under www.epo.org/fees.

8. Restoration of priority right

Where the international application contains a priority claim to an earlier application and it has been filed within two months from the expiration of the 12-month priority period, a request for restoration before the EPO as designated Office (R. 49ter.2 PCT) applies under the following circumstances:

- a) No request for restoration filed before the receiving Office (RO) during the international phase (R. 26bis.3 PCT)
- b) Negative decision by the RO irrespective of the criterion applied (due care/ unintentionality)
- c) Positive decision by the RO based on the unintentionality criterion.

For a request to be admissible, it must be filed and the requisite fee must be paid (R. 49ter.2(b)(iii) and R. 49ter.2(d) PCT). Attention is drawn to the one-month time limit under R. 49ter.2(b)(i) PCT for filing the request, which starts from the expiry of the 31-month time limit pursuant to Rule 159(1)EPC and Article 22(3) or 39(1)(b) PCT or, where applicable, from the date on which an effective request for early processing pursuant to Article 23(2) or 40(2) PCT is filed with the EPO as a designated/elected office ('Notice from the European Patent Office dated 21 February 2013 concerning the request for early processing', OJ EPO 2013, 158). The request for restoration also needs to state the reasons for the failure to file the international application within the priority period (Rule 49ter.2(b)(ii) PCT).

9. If the applicant had appointed a representative during the application's international phase, the present Form will be sent to the representative, asking him to inform the applicant accordingly.
All subsequent communications will be sent to the applicant, or - if the EPO is informed of his appointment in time - to the applicant's European representative.
10. For more details about time limits and procedural acts before the EPO as designated or elected Office, see the EPO brochure "How to get an European patent", Guide for applicants - Part 2, PCT procedure before the EPO - "Euro-PCT" (EPO PCT Guide). This brochure, the list of professional representatives before the EPO, Form 1200 and details of the latest fees are available on the Internet under <http://www.epo.org>.

11. Programme for accelerated prosecution of European patent applications - "PACE"

Applicants wishing to accelerate proceedings before the EPO as designated or elected Office may request accelerated search and/or examination under the PACE programme (Notice from the European Patent Office dated 4 May 2010 concerning the programme for accelerated prosecution of European patent applications - "PACE", OJ EPO 2010, 352). To be as effective as possible, this should preferably be requested immediately on entry into the European phase.

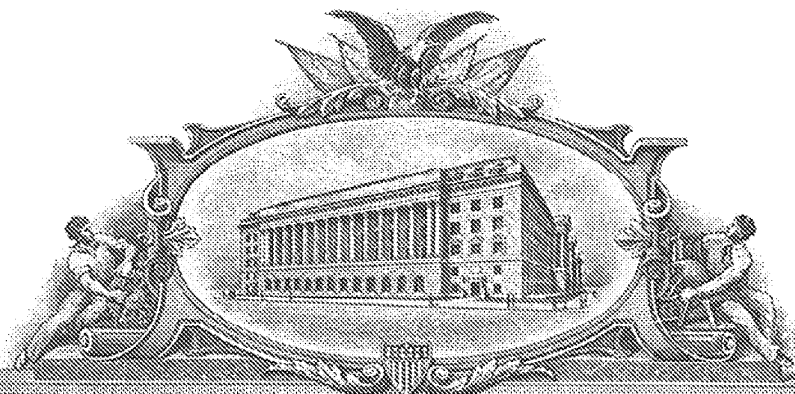
Receiving Section

**DOCUMENT MADE AVAILABLE UNDER THE
PATENT COOPERATION TREATY (PCT)**

International application number:	PCT/US2014/036832
International filing date:	05 May 2014 (05.05.2014)
Document type:	Certified copy of priority document
Document details:	Country/Office: US
	Number: 61/819,470
	Filing date: 03 May 2013 (03.05.2013)
Date of receipt at the International Bureau:	09 June 2014 (09.06.2014)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a),(b) or (b-bis)

630814



THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

June 08, 2014

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE.

APPLICATION NUMBER: *61/819,470*

FILING DATE: *May 03, 2013*

RELATED PCT APPLICATION NUMBER: *PCT/US14/36832*

THE COUNTRY CODE AND NUMBER OF YOUR PRIORITY APPLICATION, TO BE USED FOR FILING ABROAD UNDER THE PARIS CONVENTION, IS *US61/819,470*



Certified by

David S. Kybas

Under Secretary of Commerce
for Intellectual Property
and Director of the United States
Patent and Trademark Office

METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS

BRIEF DESCRIPTION OF THE DRAWINGS

- 5 **Fig. 1** depicts a first dashboard in accordance with an exemplary embodiment of the present disclosure;
- Fig. 2** depicts a second dashboard in accordance with an exemplary embodiment of the present disclosure;
- Fig. 3** depicts a third dashboard in accordance with an exemplary embodiment of the present disclosure;
- 10 **Fig. 4** depicts a fourth dashboard in accordance with an exemplary embodiment of the present disclosure;
- Fig. 5** depicts a fifth dashboard in accordance with an exemplary embodiment of the present disclosure; and
- 15 **Fig. 6** depicts a sixth dashboard in accordance with an exemplary embodiment of the present disclosure.

DESCRIPTION

- 20 The Webroot Sensor Agent provides visibility into occurrences across an environment to ensure that an administrator is aware of any system changes and data communication in and out of their devices. In this implementation, there are five components, or modules, involved in the event gathering and processing: the low level system filters, the local aggregator and interpreter, the context analyzer, global perspective, and the event distributor.
- 25 The system filters are 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
- 30 that they do not impact system performance, a key aspect of this solution; a product which impacts system performance will have considerably diminished value to an

administrator and can negatively affect the results of its own analysis. 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. In embodiments, events are gathered and timestamped 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, collecting them in batches from the queues in which they are inserted in realtime, and transmits them to the local service process where they 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. 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.

5 One goal of the context analyzer is to ensure that the user looks at 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. Conventional products in this space receive events outside of the system (for example, as
10 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.

15 After the contextual analysis completes, the 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
20 the overhead generally associated with the complex rule processing within the overall database – the additional layer may be named SkyMD5). 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,
25 assessing the reputation and category of each website and IP address as they are contacted.

The event distributor may batch and transmit the events to the end recipient after the global perspective has been applied. In one implementation, the syslog protocol is used to send each event as a line of log data to be processed by an end consumer –
30 usually a display/query engine like the product “splunk”. 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, the transmission engine builds the final line, packages it together with information about the host itself, and then sends it directly into a separate queue where it will then be sent shortly after
5 (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 like “splunk” or using other proprietary software, can display and view single events or perform wider analysis on groups of events, producing dashboard views and graphs to aid the
10 administrator in identifying events that are most pertinent to their current investigation. The dashboards developed to be run on top of Splunk software may be written in XML language and may follow Splunk development guidelines.

In regards to Figures 1-6, the dashboards generally correlate all the events collected by a Webroot sensor agent - File System/Disk activity, network activity,
15 registry activity on the endpoint - along with the Webroot Global Community data and Brightcloud IP and domain reputation data to provide a complete point of view of the system activity and further provide a full meaning to every single reported event. This results in spotting and highlighting behaviours in the endpoints that could be potentially generated by malicious activity.
20 Each dashboard provides a specific heuristic that targets a specific potential malicious behaviour.

The dashboard of Figure 1, generally looks for executables that have been found and executed from specific critical paths in the system - those paths that are known to host malware executables (browser's cache, temporary files folder, system32 folder, auto
25 start folder and so on). The dashboard may filter for files determined as good, unknown and bad from the Webroot global community. For unknown files, the dashboard may show their popularity on the Webroot Global Community - i.e. on how many PCs they have been seen - and if they establish outbound internet connections. If the files connect to the Internet, the dashboard may trace down and identify the specific connection and
30 geo-locate the destination address on a world map.

The dashboard of Figure 2 generally analyses outbound connections from the analysed endpoints. The dashboard may filter out and highlight connections to high-risk countries - those countries known to host malicious servers - and it 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 those connections may be shown on a map view and the contacted IPs and domains are crosschecked with a BrightCloud database to determine their reputation and website category (if known).

The dashboard of Figure 3 highlights potential exploits detected on the endpoint by monitoring the most common software usually installed on an average PC and targeted by exploit attacks. The dashboard generally identifies software like Java, Adobe Acrobat, Microsoft Office, Flash Player and monitors if they are dropping executable files on the system; if they behave in this manner, this should be considered a suspicious behaviour, as they are not supposed to drop and execute any executable file on the system. If something is detected, the dashboard analyses the dropped executable for its popularity in the Webroot global community and then identifies potential outbound connections established by the just-dropped executable. If an outbound connection is found, the dashboard retrieves the destination IP and draws it on a map view, such as a world map.

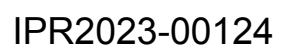
In the dashboard of Figure 4, highlighted are those new processes created on the monitored endpoints that are undetermined and have only been recently seen in the Webroot global community. For every process, a lifetime scheme is assembled which allows the admin to understand when the undetermined file 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.

The dashboard of Figure 5 highlights 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 are suspected of hosting malicious code, the malicious code having been injected into them. For every established connection, the dashboard traces and identifies the contacted country and the specific IP/domain.

The dashboard of Figure 6 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
5 storage location.

What is claimed is:

1. A method comprising:
gathering one or more system events;
5 generating a contextual state for the one or more system events by correlating the one or more system events to at least one object, the object comprising at least one of an originating process, device, and user;
obtaining information associated with the object, the information comprising at least one of age, popularity, and a status; and
10 transmitting the one or more system events and the information associated with the object to an end recipient.
2. The method of Claim 1, further comprising:
caching the one or more system events; and
15 asynchronously consolidating and normalizing the one or more system events.
3. The method of claim 1, further comprising:
correlating the one or more system events and the at least one object; and
heuristically displaying the correlated one or more system events and the at least
20 one object according to one or more of (i) a location associated with the object; (ii) at least one characteristic of an outbound connection associated with the object; (iii) a dropped executable file; (iv) an age of the object; and (v) a number of concurrent connections associated with the object.



Iberian lynx distribution in 1996

Area	Population	Reproduction	Survival	Status
Iberian Peninsula	1,000	1.0	0.5	Endangered

Iberian lynx distribution in 2006

Area	Population	Reproduction	Survival	Status
Iberian Peninsula	100	0.5	0.2	Critically Endangered

IPR2023-00124
CrowdStrike EX1032 Page 165

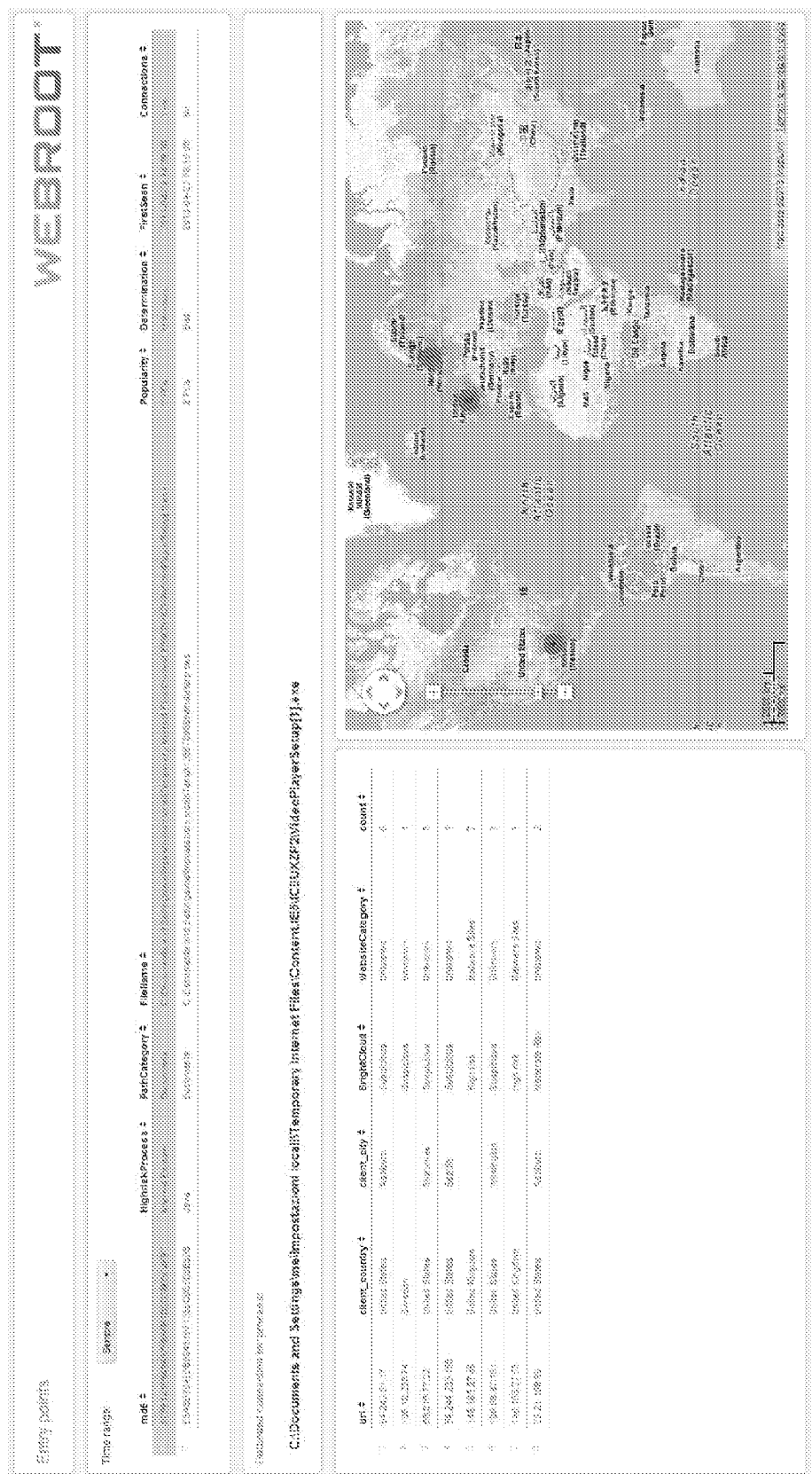
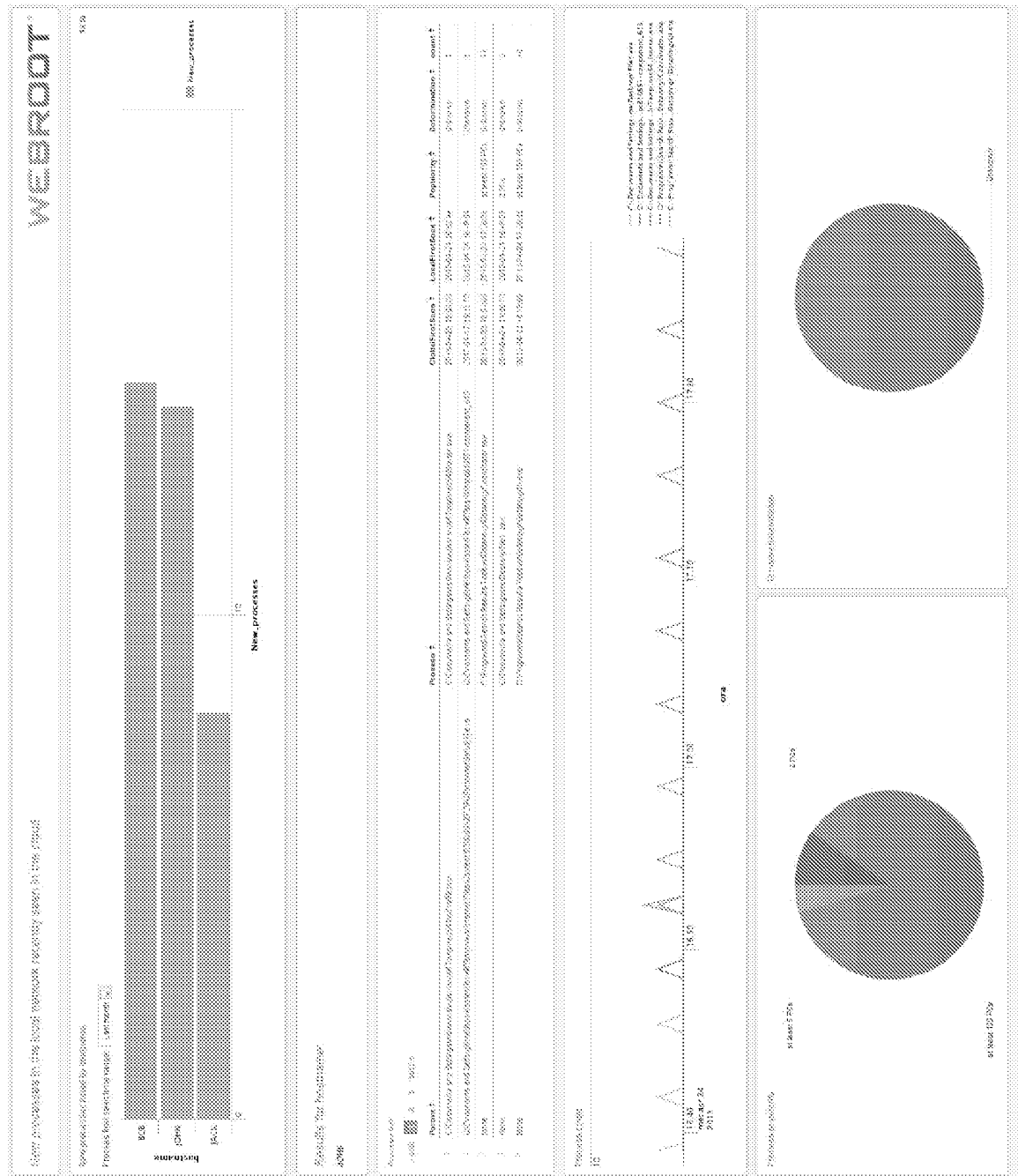
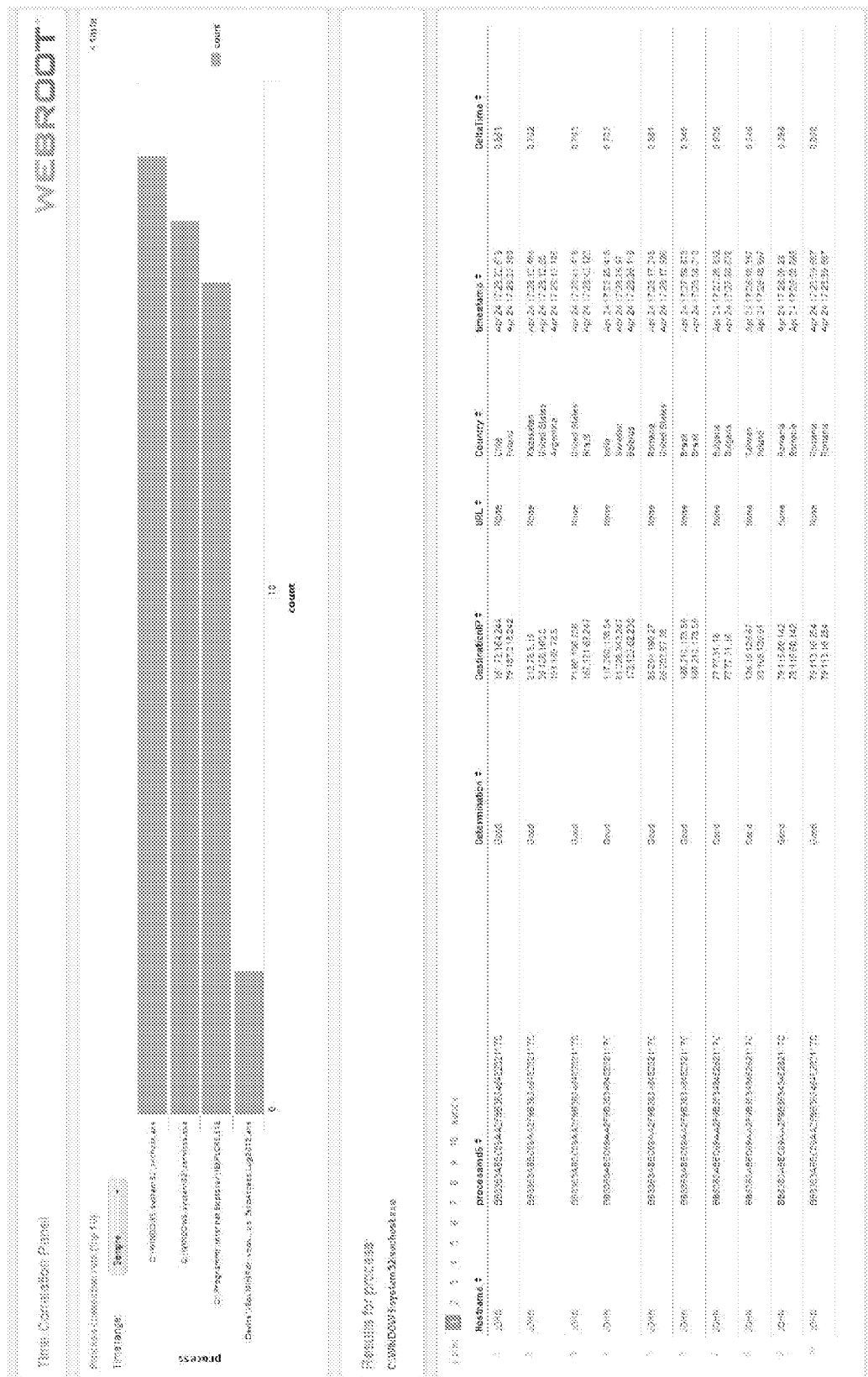
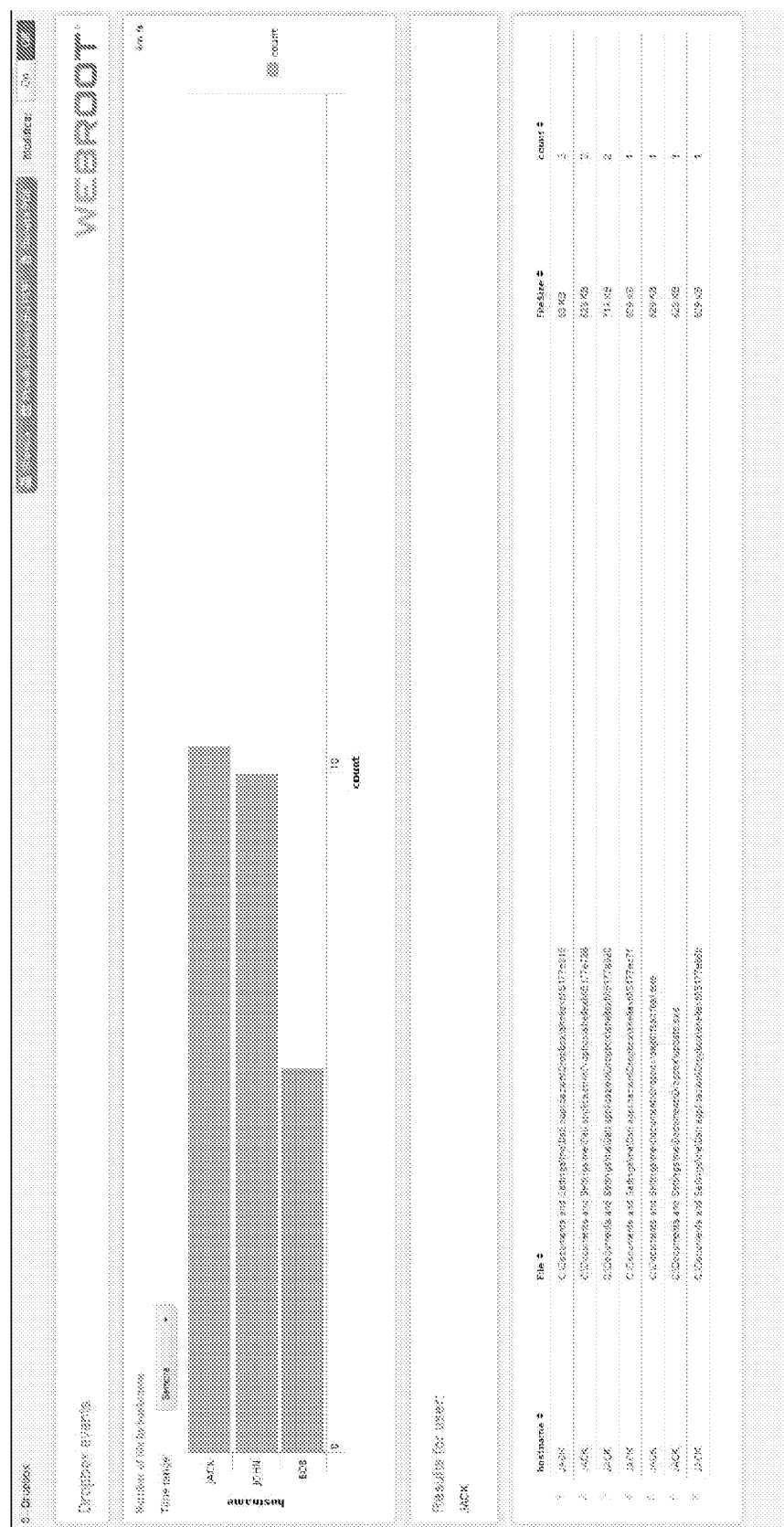


FIGURE 3







Doc Code: **TR.PROV**

Document Description: Provisional Cover Sheet (SB16)

PTO/SB/16 (11-08)

Approved for use through 05/31/2015. OMB 0651-0032

U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

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

Provisional Application for Patent Cover Sheet					
This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c)					
Inventor(s)					
Inventor 1					Remove
Given Name	Middle Name	Family Name	City	State	Country
Joseph	A.	JAROCK	Deer Park	IL	US
Inventor 2					Remove
Given Name	Middle Name	Family Name	City	State	Country
Jacques	Etienne	ERASMUS	Belper		UK
Inventor 3					Remove
Given Name	Middle Name	Family Name	City	State	Country
Paul		BARNES			UK
Inventor 4					Remove
Given Name	Middle Name	Family Name	City	State	Country
Johannes		MAYR			AT
Inventor 5					Remove
Given Name	Middle Name	Family Name	City	State	Country
Michael		LIEDESDORFF	Niwot	CO	US
Inventor 6					Remove
Given Name	Middle Name	Family Name	City	State	Country
Marco		GIULIANI	Bastia Umbra		IT
Inventor 7					Remove
Given Name	Middle Name	Family Name	City	State	Country
Marco		BIZZARRI	Sassoferrato		IT
Inventor 8					Remove
Given Name	Middle Name	Family Name	City	State	Country
Benedetto		VOLTATTORNI	San Benedetto 		IT

Doc Code: **TR.PROV**

Document Description: Provisional Cover Sheet (SB16)

PTO/SB/16 (11-08)

Approved for use through 05/31/2015. OMB 0651-0032

U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

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

All Inventors Must Be Listed – Additional Inventor Information blocks may be generated within this form by selecting the Add button. Add	
Title of Invention	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS
Attorney Docket Number (if applicable)	6890-103-PROV
Correspondence Address	
Direct all correspondence to (select one):	
☒ The address corresponding to Customer Number	☐ Firm or Individual Name
Customer Number	22442

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.
☒ No.
☐ Yes, the invention was made by an agency of the United States Government. The U.S. Government agency name is:
☐ Yes, the invention was under a contract with an agency of the United States Government. The name of the U.S. Government agency and Government contract number are:

Doc Code: **TR.PROV**

Document Description: Provisional Cover Sheet (SB16)

PTO/SB/16 (11-08)

Approved for use through 05/31/2015. OMB 0651-0032

U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

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

Entity Status

Applicant asserts small entity status under 37 CFR 1.27 or applicant certifies micro entity status under 37 CFR 1.29

- ☒ Applicant asserts small entity status under 37 CFR 1.27
- ☐ Applicant certifies micro entity status under 37 CFR 1.29. Applicant must attach form PTO/SB/15A or B or equivalent.
- ☐ No

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 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.

Signature

Please see 37 CFR 1.4(d) for the form of the signature.

Signature	/Brent R. Lindon/			Date (YYYY-MM-DD)	2013-05-03
First Name	Brent	Last Name	Lindon	Registration Number (If appropriate)	67424

This collection of information is required by 37 CFR 1.51. 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 8 hours 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. **This form can only be used when in conjunction with EFS-Web. If this form is mailed to the USPTO, it may cause delays in handling the provisional application.**

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:	15691602
Application Number:	61819470
International Application Number:	
Confirmation Number:	9817
Title of Invention:	METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS
First Named Inventor/Applicant Name:	Joeseeph A Jaroch
Customer Number:	22442
Filer:	Brent Robert Lindon
Filer Authorized By:	
Attorney Docket Number:	6890-103-PROV
Receipt Date:	03-MAY-2013
Filing Date:	
Time Stamp:	19:56:36
Application Type:	Provisional

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$ 130
RAM confirmation Number	6289
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)	

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		Provisional_App_Dwg.pdf	1021371 3f53e4e0d46dd82fe9a7a4542ed609a9c22d44bc	yes	13
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Specification		1	6	
	Claims		7	7	
	Drawings-only black and white line drawings		8	13	
Warnings:					
Information:					
2	Provisional Cover Sheet (SB16)	ProvisionalSB.pdf	1477359 4513cb689faf0d0ab1b00b319f9e2726abe b7d	no	4
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30116 6e53ac731ce25aa645197b538e24be6b45e8130a	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			2528846		

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.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2014/036832

A. CLASSIFICATION OF SUBJECT MATTER IPC(8) - G06F21/00 (2014.01) CPC - H04L63/14 (2014.02) According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) IPC(8) - G06F21/00; G06F12/14; G06F11/30; H04L9/32 (2014.01) USPC - 709/224; 726/22, 23, 25 Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched CPC - H04L63/14; H04L63/1408; H04L63/1416; H04L63/1425 (2014.02) Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) PatBase, Google Patents, Google Scholar		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2012/0260340 A1 (MORRIS et al.) 11 October 2012 (11.10.2012) entire document	1-4, 7-13, 16-19
---		---
Y	US 2006/0095963 A1 (CROSBY et al.) 04 May 2006 (04.05.2006) entire document	5-6, 14-15, 20
Y	US 2006/0095963 A1 (CROSBY et al.) 04 May 2006 (04.05.2006) entire document	5-6, 14-15
Y	US 2012/0072725 A1 (FANTON et al.) 22 March 2012 (22.03.2012) entire document	20
A	US 7,895,649 B1 (BROOK et al.) 22 February 2011 (22.02.2011) entire document	1-20
A	US 2009/0300769 A1 (SRINIVASA et al.) 03 December 2009 (03.12.2009) entire document	1-20
☐ Further documents are listed in the continuation of Box C. ☐		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search 09 September 2014		Date of mailing of the international search report 29 SEP 2014
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201		Authorized officer: Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (July 2009)



- (51) International Patent Classification:
G06F 21/00 (2013.01)
- (21) International Application Number:
PCT/US2014/036832
- (22) International Filing Date:
5 May 2014 (05.05.2014)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
61/819,470 3 May 2013 (03.05.2013) US
- (71) Applicant: **WEBROOT INC.** [US/US]; 385 Interlocken
Parkway, Suite 800, Broomfield, CO 80021 (US).
- (72) Inventors: **JAROCH, Joseph, A.**; 20540 N. Westpark
Place, Deer Park, IL 60010 (US). **ERASMUS, Jacques,
Etienne**; 8 Hillcrest, Overlane, Belper DE5 60JF (GB).
BARNES, Paul; 8 Wren Way, Mickleover, Derby DE3
0UF (GB). **MAYR, Johannes**; Lederergasse 31A, A-4020
Linz (AT). **LEIDESDORFF, Michael**; 8425 Firethorn
Court, Niwot, CO 80503 (US). **GIULIANI, Marco**; Via

Santa Elisabetta 21C, I-06083 Bastia Umbra (PG) (IT).
WILLIAMS, Christopher, John; 28 William Brown
Square, Chesterfield, Derbyshire S40 2FX (GB). **BACH-
ER, Chad, Edward**; 13328 W. 87th Terrace, Arvada, CO
80005 (US).

(74) Agent: **LINDON, Brent, R.**; Sheridan Ross P.C., 1560
Broadway, Suite 1200, Denver, CO 80202 (US).

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

(84) Designated States (unless otherwise indicated, for every
kind of regional protection available): ARIPO (BW, GH,

[Continued on next page]

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

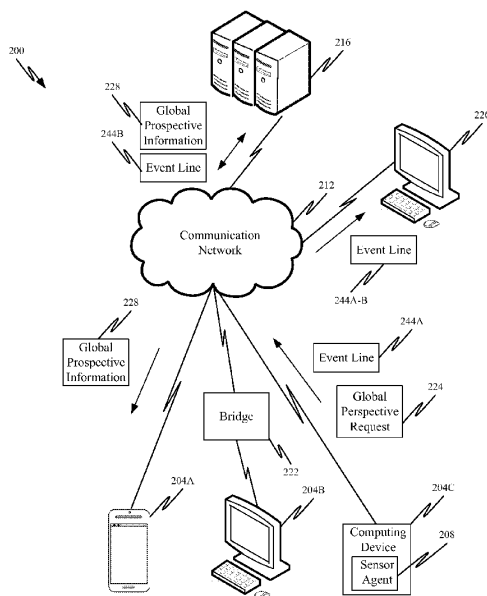


Figure 2

(57) Abstract: Methods and systems for providing forensic visibility
into systems and networks are provided. More particularly, a sensor
agent may receive events defining an action of a first object acting on
a target. The object, the event, and the target are then correlated
to at least one originating object such that an audit trail for each in-
dividual 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 ap-
plied to at least one of the object, the event, the target, and the ori-
ginating object. A priority may then be determined and assigned to
the event based on at least the global perspective. An event line con-
taining event information is then transmitted to an end recipient
where the information may be heuristically displayed.



GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

- *with international search report (Art. 21(3))*
- *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

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,
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
20 disk or to a database over the network.

 However, existing network forensic tools, such as network sniffers and packet
capturing tools, passively collect information about network traffic. Such tools may be
able to detect and capture information associated with communication sessions, such as
hostnames, ports, protocols, IP addresses, etc.; however, such tools tend to receive
25 network events outside of a host or system. That is, a network forensic tool, such as a
network sniffer, may reside at a network edge and may receive network events concerning
the network from one or more hosts or systems. Accordingly, network edge devices have
no ability to establish any sort of context from within the host or system that is generating
the event. Therefore, devices residing at a network edge may monitor, record, and or
30 analyze network traffic between the host and the device, but information that may be
useful within the host is not obtained.

 For example, Figure 1 generally illustrates a comparative example including
computing devices 104 and 108 in communication with a network edge device 116. The
network edge device 116 may be commonly referred to as a “sniffer” which may monitor,

capture, and analyze network traffic between the network edge device 116 and the computing devices 104 and 108. The network edge device 116 may further be in communication with a communication network 124, such as the internet. Accordingly, the network edge device 116 may monitor, capture, and analyze network traffic between the computing devices 104 and 108 and between the computing devices 104/108 and the communication network 124.

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

SUMMARY

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

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

20 In at least one embodiment, the second component, the local aggregator and interpreter, receives events from the low level system filters, collecting them in batches from the queues in which they are inserted in real-time, and transmits these events to a local service process where the events are held for further analysis. At this stage, intelligent caching may be invoked to drop events which are duplicates of recent events,
25 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
30 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.

5 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
10 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
15 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
20 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
25 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
30 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;

- 5 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
10 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
15 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
20 malware; and Internet Protocol (IP) Address or Uniform Resource Locator (URL) information; assemble an event line including details associated with the at least one event, the details including information uniquely identifying each of the first object, the action of the first object, the target, and the originating object; and transmit the assembled event line utilizing the communication interface.

25 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
30 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.

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

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

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

BRIEF DESCRIPTION OF THE DRAWINGS

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

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

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

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

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

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

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

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

10 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;

15 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

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

DETAILED DESCRIPTION

Figure 1 depicts aspects of a system 200 for providing forensic visibility into one or more computing devices 204, 208, and 212 in accordance with at least one embodiment of the present disclosure. In general, the system 200 includes one or more computing
25 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
30 presenting content to an associated user. The computing device 204 may also comprise a processing unit that is interconnected to an affiliated input/output device.

The communication network 212 may include one or more networks capable of supporting communications between nodes of the system 200, including but not limited to a computing devices 204A-C, the global perspective information server 216 and the end

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

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

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

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

Table 1:

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

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

The second component, the local aggregator and interpreter, receives events from the low level system filters in batches from the queues in which they are inserted in real-time, and transmits them to the local service process where they are held for further

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

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

After the contextual analysis completes, the sensor agent 208 establishes a global perspective for each event by calling on the global perspective information server 224. For example, the sensor agent 208 of the computing device 204 may determine if global perspective information is available locally within a cache. If the global perspective

information is not available locally, the sensor agent 208 of the computing device 204 may issue a global perspective request 224 utilizing the communication network 212 and destined for the global perspective information server 216. The global perspective information server 216 may respond with global prospective information 228 and such
5 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, and/or IP/URL information. Not all information may be provided by the global
10 perspective 228; that is, the global perspective 228 may include age information, popularity information, good, bad, or unknown determination, or IP/URL information. Alternatively, or in addition, the global perspective 228 may include combinations of information, such as age and popularity information, popularity and known good, bad, or unknown determinations, or age and known good, bad, or unknown determination
15 information. Or, the global perspective 228 may include IP/URL information. 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
20 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
25 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
30 reputation be assigned an event priority representative of a potential risk assigned to the computing device 204 and/or network. Accordingly, when the event line containing event priority information is received at an end recipient 220, the end recipient 220 may be able to more easily identify events, and/or instances of malware, that require more immediate attention.

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

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

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

Figure 3 illustrates additional aspects of a system 200 in accordance with embodiments of the present invention, and in particular illustrates additional features and components of a computing device 204 and a bridge 222. The computing device 204 may comprise a general purpose computer, tablet computer, smart phone, or other device or federated group of devices capable of supporting communications over a communication network 212. The computing device 204 may include a processor 316, memory 304, one or more user input devices 308, such as a keyboard and a pointing device, and one or more user output devices 312, such as a display, speaker, and/or printer. Alternatively, or in addition, the user input 308 and the user output 312 may be combined into one device,

such as a touch screen display. Computing device 204 may further include a communication interface 328 for communicating with another computing device 204, a global perspective information server 216, an end recipient 220, and/or the communication network 212.

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

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

- 25 The data storage 320 may generally include storage for programs and data. For example, data storage 320 may provide storage for a sensor agent 208 including the system filters 340, the local aggregator and interpreter 344, the context analyzer 348, the global perspective module 352, the event distributor 356, and/or the general operating system and other programs and data 324. Additionally, the data storage 320 may also
- 30 include an event store 328, such as a database, for storing and/or caching event information, context information, global perspective information, and/or event lines. One or more components of the computing device 204 may communicate with one another utilizing a bus 336. Alternatively, or in addition, the sensor agent 208 may be provided separate and apart from data storage 320. That is, the sensor agent 208, including the

system filters 340, the local aggregator and interpreter 344, the context analyzer 348, the global perspective module 352, the event priority generation unit 358, and the event distributor 356 may be implemented using a processor, such as a microprocessor 304. Accordingly, the microprocessor 304 may be specifically programmed to carry out one or more functions of the sensor agent 208. For example, the processor 304 may execute instructions associated with the sensor agent 208, including the system filters 340, the local aggregator and interpreter 344, the context analyzer 348, the global perspective module 352, the event priority generation unit 358, and the event distributor contained within memory 304 and/or storage 320. Alternatively, or in addition, the sensor agent 208, including the system filters 340, the local aggregator and interpreter 344, the context analyzer 348, the global perspective module 352, the event priority generation unit 358, and the event distributor 356 may share the processor 304.

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

The local aggregator and interpreter receives events from the system filters 340, and collects the received events into batches from the queues in which they are inserted in real-time. The batches of events are then transmitted to a local service process where the events are held for further analysis. Such events may be held, or otherwise stored, within an event store 328. At this stage, intelligent caching may be invoked to drop events which are duplicates of recent events, and some data normalization may be performed to ensure consistency. Caching may be implemented sparingly but in critical areas to ensure redundant events are not continually reported – many applications perform thousands of the same events (network access to the same destination IP address, for example) and transmitting these events into an external log source would create a significant amount of unnecessary noise and potential performance degradation. The cache may integrate a “time to live” concept to prevent applications from hiding their traffic within their noise. For example, events meeting predefined criteria may be dropped from the real-time system event queues. In some embodiments, if the predefined criteria include determining if a

system event is the same or otherwise matches a previous system event, then the event may be dropped. Additionally, if a duplicate event occurs within a specified time, the event may be dropped from the queue. Alternatively, or in addition, if the duplicate system event occurs within a specified period of time, the duplicate system event may be modified to reflect that the duplicate system event is the same as a previously occurring system event. Accordingly, the later occurring duplicate system event may receive all contextual state information and global perspective information without requiring all of the determinations and/or lookups of such information. However, a time-to-live (TTL) functionality may be implemented on a cache basis to ensure that cached events, or previous events having context and/or a global perspective, are current. Accordingly, not all previous events having contextual information may be available to provide contextual information to a current event. As another option, the later occurring duplicate system event may be modified in a manner such that when the later occurring duplicate system event is interpreted by the end recipient 220, the end recipient 220 may determine that the system event information may be the same as a previously parsed system event line. Accordingly, a full event line for the duplicate system event is not generated and/or transmitted saving bandwidth and information processing resources. Further, the caches may automatically roll over to ensure sufficient space is always available without requiring exorbitant amounts of memory.

The local aggregator and interpreter 344 may additionally perform data normalization on items such as kernel filenames, user mode filenames, process objects, registry objects, and other system structures and normalizes them into a standard format which is easy more easily consumed by automated parsers. Consolidating and normalizing data at this stage allows the data to be handled much more quickly at the higher levels to avoid reprocessing data and potentially missing events just because they were referred to slightly differently (\Device\HarddiskVolume1\Windows\file.exe instead of C:\Windows\file.exe for example). In some embodiments, an aspect of this subsystem provides the ability to process events asynchronously. The subsequent modules which will execute over the data may potentially take a considerable amount of time to complete but delaying the response for each event at this phase would result in a significant system slowdown. Instead, events are intelligently queued in multiple layers to minimize the number of individual threads but still ensure each event is given sufficient time to be independently processed. Because of this structure, there is little to no performance

difference if an event takes one millisecond to be processed or one hour for the full series of routines to complete.

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

After the context analyzer completes, the sensor agent 208 may attempt to establish a global perspective for each event by calling the cloud database utilizing an infrastructure similar to the infrastructure discussed in U.S. Application Serial No. 13/372,375 filed February 13, 2012, "Methods and Apparatus for Dealing with Malware" (US-2012-0260340-A1, but with an additional layer capable of responding in a highly scalable manner which avoids the overhead generally associated with the complex rule processing within the overall database. Such an additional layer may be named SkyMD5. The response from the SkyMD5 layer may include information related to the age, popularity, and determination of an object – whether it is known good, bad, or unknown. This data may then be normalized and appended to each relevant portion of the event line. Further lookups are performed for network activity, assessing the reputation and category of each website and IP address as they are contacted.

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

contextual state information may only be available locally for a specified period of time and/or specified number of system events.

The event priority module 358 may contain priority logic, or one or more rule sets, to associate a priority to one or more events. The event priority module may utilize
5 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
10 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
15 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
20 transmission engine of the event distribute 356 builds the final event line, packages the event line together with information about the host itself, and then sends it directly into a separate queue where it will then be sent shortly after (usually a few seconds) while maintaining the pre-set timestamp of precisely when the event took place even if it is sent several seconds later. The separate queue may be a queue located in the storage data 320
25 and more specifically in the event store 328.

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

or similar as that which was described with respect to processor 316 and memory 304 respectively.

The data storage 370 may generally include storage for programs and data. For example, data storage 370 may provide storage for a cached event store 394 and/or the
5 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
10 bridge 222 may aggregate communications to and from one or more computing system 204 such that information to and from sensor agent 208 is cached and stored at the cached event store 394, optimizing global perspective requests and other communications. Additionally, the bridge 222 may perform selective or intelligent caching of global perspective information such that subsequent lookups or requests of global perspectives
15 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
20 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
25 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.

30 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.

5 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
10 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
15 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
20 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
25 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
30 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
5 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
10 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
15 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
20 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
30 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 be determined based on a previous event that initiated or otherwise created the current process and/or object. Additionally, as illustrated in Figure 5B, the GenesisActor is determined based on a chain of previous events. For example, the Actor of Object 1 for system event 504B of Event Type “executes” operates on Filename 1. Object 1 subsequently creates a process Object 2 in 508B which is further utilized in both 516B and 520B. Accordingly, as the Object 1 initiated subsequent events, Object 1 may be determined to be the GenesisActor for 520B, 516B, 512B, and 508B.

As illustrated in Figure 5C, a global perspective is applied to event 520C. The global perspective may comprise information for each object in the event and/or the contextual state 524. For example, a global perspective may be obtained for Object 2, Object 3, and Object 1 as illustrated. Accordingly, a global perspective 528 indicating the age of Object 2, the popularity of Object 2, the determination of Object 2, and/or additional IP/URL information of Object 2 may be provided. Similar global perspective

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

Referring now to Figure 6, a method 600 for providing forensic visibility into a system is provided in accordance with embodiments of the present disclosure. Method
10 600 is in embodiments, performed by a device, such as the sensor agent 204 and/or the end recipient 220. More specifically, one or more hardware and software components may be involved in performing method 600. In one embodiment, one or more of the previously described units perform one or more of the steps of method 600. The method 600 may be executed as a set of computer-executable instructions executed by a computer system and
15 encoded or stored on a computer-readable medium. Hereinafter, the method 600 shall be explained with reference to systems, components, units, software, etc. described with Figures 1-5C.

Method 600 may continuously flow in a loop, flow according to a timed event, or flow according to a change in an operating or status parameter. Method 600 is initiated at
20 step 604 where events of a computing system 204 may be initiated. At step 608, such an event may be detected. As previously discussed, the events, which may comprise system events, may be detected by one or more system filters 340 of a sensor agent 208. The sensor agent 208 may be comparatively small compared with other commercially available forensic tools and anti-malware software. This may be achieved by the sensor agent 204
25 being developed in a low-level language, having direct access to system resources such as the video display, disk, memory, the network(s), and without the incorporation of many standard code or dynamic linked libraries to perform these functions. Memory usage may be optimized by storing data in a local database structure that provides the ability to refer to objects by a unique identifier rather than requiring full filenames or signatures. All
30 unnecessary dynamic link libraries are unloaded from the process immediately as they are identified as no longer being used, and background threads are merged to reduce CPU usage. A small, efficient sensor agent 204 may be deployed more quickly and may be used alongside other programs, including other security programs, with less load on or

impact on the computer's performance. This approach also has the advantage of having less surface area for attack by malware making it inherently more secure.

Method 600 then proceeds to step 612 where the local aggregator and interpreter 344 receives events from the low level system filters 340, collecting them in batches from the queues in which they are inserted in real-time. As previously discussed, intelligent caching may be invoked to drop events which are duplicates of recent events. Further, some data normalization may be performed at step 612 to ensure consistency. Further still, caching may be implemented sparingly but in critical areas to ensure redundant events are not continually reported. Method 600 then proceeds to step 616 where a contextual state may be applied by a context analyzer 348 to the event information. Accordingly, the context analyzer correlates events to objects such that an audit trail for each individual event is created. As a contextual state is established, it is cached and aggregated to be quickly queried in subsequent lookups further reducing latency and improving the responsiveness of the system. Once a contextual state is applied, method 600 then proceeds to step 620 where a global perspective is applied for each event and/or each object of the event and contextual state. Accordingly, information related to the age, popularity, and determination of an object – whether it is known good, bad, or unknown is obtained. In addition, as previously mentioned, the global perspective may contain information pertaining specifically to an IP/URL address. For example, the global perspective may include information relating network activity and an assessment of the reputation and category of each website and IP address as they are contacted. This data may then be normalized. Method 600 then proceeds to step 622 where an event priority may be applied to the event. As previously discussed, the event priority may be obtained utilizing a rule set and applying such a rule set to aggregated event information, contextual state information, and global perspective information. Accordingly, method 600 then proceeds to step 624 where such data is appended to each relevant portion of an event line.

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

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

10 Method 700 may continuously flow in a loop, flow according to a timed event, or flow according to a change in an operating or status parameter. Method 700 is initiated at step 704 where events of a computing system 204 may be initiated. At step 708, such an event may be detected. As previously discussed, the events, which may comprise system events, may be detected by one or more system filters 340 of a sensor agent 208.
15 Accordingly, at step 712, an event record may be created. The event record may be the same or similar to that which was described with respect to Figure 5A. Accordingly, the event record may include an Event ID, and Event Type, an Actor, and a Victim. Moreover, in some embodiments, instead of creating a separate event record and a separate event line, a single event line for each event may be utilized. That is, the event
20 record may be the event line. Accordingly, at step 716 the event line and/or the event record may be time stamped and stored. At step 720, method 700 may then determine which queue the event record or event line, should be assigned. In some embodiments, the event record/event line may be assigned to a specified queue based on the event type. Alternatively, or in addition, the event record/event line may be assigned to a specified
25 queue based on the needed resources and the available resources. Method 700 then ends at step 724.

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

computer-readable medium. Hereinafter, the method 800 shall be explained with reference to systems, components, units, software, etc. described with Figures 1-7.

Method 800 may continuously flow in a loop, flow according to a timed event, or flow according to a change in an operating or status parameter. Method 800 is initiated at
5 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 previous event record/event line, method 800 may proceed to step 824 where the current
10 event record/event line may be dropped. Alternatively, or in addition, the dropped event record/event line may be modified such that either the contextual analyzer 348 and/or the global perspective unit 352 may be able to determine a contextual state and global perspective based on a previously captured event record/event line. Alternatively, or in addition, the dropped event record/event line may be modified to refer to a previously
15 captured event record/event line such that upon parsing by the end recipient 220, the current event line/event record is provided meaning from a previously parsed event record/event line

Accordingly, method 800 may then proceed to step 816 where the information may be normalized. The normalization may be implemented with a database which takes
20 complete path names and translates them to representatives paths. So, for example, the Windows\file.exe would end up normalized to %windir%\file.exe, allowing rules to be created for any full path. Similar logic is utilized for paths like %appdata% which would have unique elements per-user and would be difficult to manage if not normalized. Accordingly, once the information in the event record/event line is normalized, method
25 800 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
30 the sensor agent 204 and/or the context analyzer 348. More specifically, one or more hardware and software components may be involved in performing method 900. In one embodiment, one or more of the previously described units perform one or more of the steps of method 900. The method 900 may be executed as a set of computer-executable instructions executed by a computer system and encoded or stored on a computer-readable

medium. Hereinafter, the method 900 shall be explained with reference to systems, components, units, software, etc. described with Figures 1-8.

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

Method 900 then proceeds to step 920 where the contextual state may be cached and made accessible for later access. In accordance with at least one embodiment, the event line may be partially assembled where the partially assembled event line may
20 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
25 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
30 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.

5 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
10 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.

15 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
20 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
25 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
30 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.

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

In at least one embodiment, the priority level may be derived from aggregated and interpreted event information from the local aggregator and interpreter 344, context analyzer 348, and global perspective unit 352. Accordingly, an event having a specified Actor, Victim, Target, originating process, or the like together with a global perspective
20 indicating that at least one of the Actor, Victim, Target, origination process has been determined to be malware may result in a rule set that assigns a priority level to the event indicating that such the event should be immediately brought to the attention of an administrator. Accordingly, the event may be said to have a "high" priority or be a "high" priority event. Method 1100 may then end at step 1116. With reference to Figure 12,
25 details of a data structure 1200 will be described in accordance with embodiments of the present disclosure. In some embodiments, the data structure 1200 may be used as an event line and may contain details specific to an event, context, and global perspective. For example, an event line 1204 may generally include, without limitation, event information 1208, a time stamp 1212, context state information 126, global perspective information
30 1220, and a priority level 1222, where the priority may be a value that ranges between a low and a high number. In some embodiments, the event field 1208 may further include Event ID information 1224, Event Type information 1228, Actor 1232, and Victim information 1236. In some embodiments, the context state 1216 may include, without limitation, Originating Process 1240 information, Device information 1244, User

information 1248, dependent data such as, but not limited to additional meta data and/or ancillary data describing or containing detailed information about one or more objects 1252, and object info 1256. In addition, the global perspective field may include, but is not limited to an age 1260, popularity 1264, malware determination 1268, and/or IP/URL information 1272, where IP/URL information may include, but is not limited to a categoryID of the IP/URL, a confidence of such a categoryID, a reputation, geolocation information such as which country the IP/URL is associated with, and/or a threat history associated with the IP/URL. Of course, additional relevant information may be included in the event line 1204 depending on the event.

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

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

In another embodiment, a separate dashboard 1336 may analyze outbound connections from the analyzed endpoints. Accordingly, this dashboard may filter out and highlight connections to high-risk countries, i.e. those countries known to host malicious servers, and retrieve software that actually established the suspicious connections. The dashboard 1336 may also provide another point of view; that is, the dashboard 1336 may highlight all connections to specific IPs and domains that have been set up recently (e.g. in the last 60 days). All connections may be shown on a map view and the contacted IPs and domains are crosschecked with a database to determine their reputation and website category (if known).

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

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

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

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

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

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

The foregoing discussion of the invention has been presented for purposes of illustration and description. Further, the description is not intended to limit the invention to the form disclosed herein. Consequently, variations and modifications commensurate with the above teachings, within the skill or knowledge of the relevant art, are within the scope of the present invention. The embodiments described hereinabove are further

intended to explain the best mode presently known of practicing the invention and to enable others skilled in the art to utilize the invention in such or in other embodiments and with various modifications required by the particular application or use of the invention. It is intended that the appended claims be construed to include alternative embodiments to
5 the extent permitted by the prior art.

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;
 - obtaining a global perspective for the at least one event by obtaining information
 - 10 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,
 - 15 the details including information uniquely identifying each of the first object, the action of the first object, the target, and the originating object; and
 - transmitting the assembled event line.
2. The method of claim 1, wherein the information associated with the one or more of the first object and the originating object is obtained from a community database;
- 20 and
 - wherein the event line is transmitted to an end recipient.
3. The method of claim 1, further comprising:
 - obtaining an event priority based on one or more of the generated context and the global perspective for the at least one event, wherein the event line further includes the
 - 25 event priority for the at least one event.
4. The method of claim 1, wherein the at least one event includes information uniquely identifying the object performing the action, information uniquely identifying the action being performed, and information uniquely identifying the target upon which the act is being performed.
- 30 5. The method of claim 4, further comprising:
 - determining whether a global perspective for the at least one event has been cached;
 - when the global perspective for the at least one event has been cached, obtaining a global perspective for the at least one event based on the cached global perspective; and

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

6. The method of claim 5, further comprising:

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

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

7. The method of claim 4, further comprising:

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

8. A computer readable storage medium comprising processor executable
15 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;

20 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
25 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;

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

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

transmit the assembled event line utilizing the communication
5 interface.

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

11. The system of claim 9, further comprising:
a global perspective information server; and
10 an end recipient device, wherein the information associated with the one or more of the first object and the originating object is obtained from the global perspective information server and the sensor agent transmits the event line to the end recipient.

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

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

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

15. The system of claim 14, wherein the sensor agent is further operable to:
determine whether the cached global perspective for the at least one event has
expired; and

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

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

with the first object; at least one characteristic of an outbound connection associated with the first object; a dropped executable file; an age of the first object; and a number of concurrent connections associated with the first object.

17. A system for providing forensic visibility into a system, comprising:
- 5 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,
- 10 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
- 15 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
- 20 transmit the assembled event line utilizing the communication interface.
18. The system of claim 17, further comprising a global perspective information server including:
- a processor;
- 25 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
- 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, the action of the first object, the target, and the originating object; and

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

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

20. The system of claim 17, further comprising a bridge including:
15 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;

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

25 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.

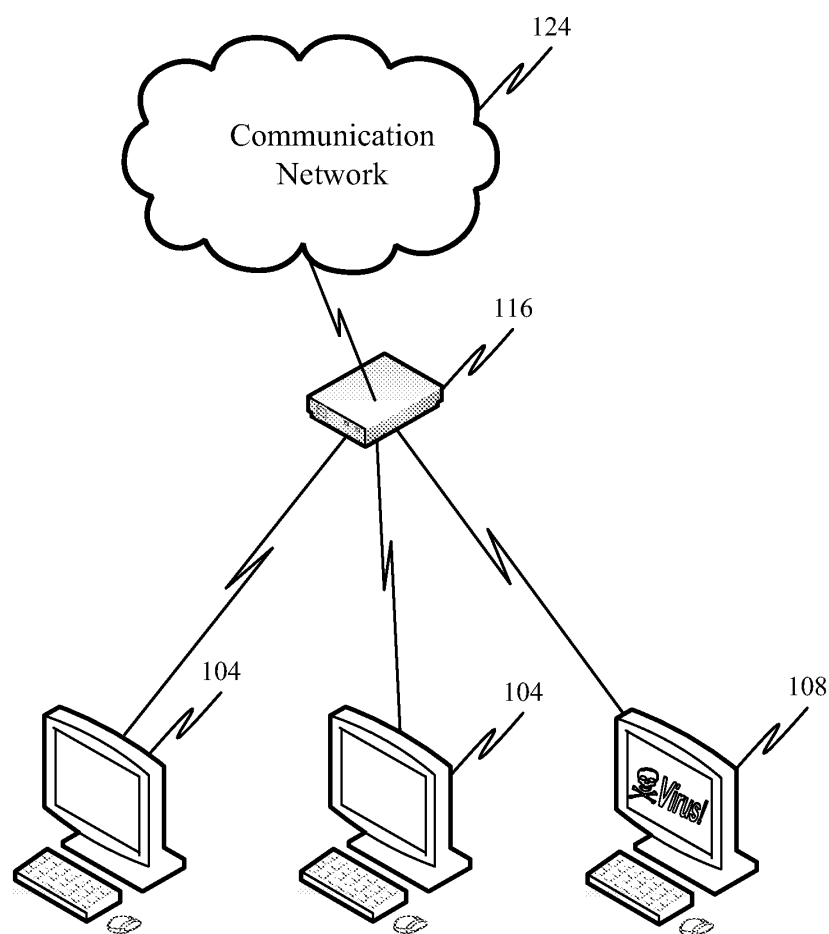


Figure 1

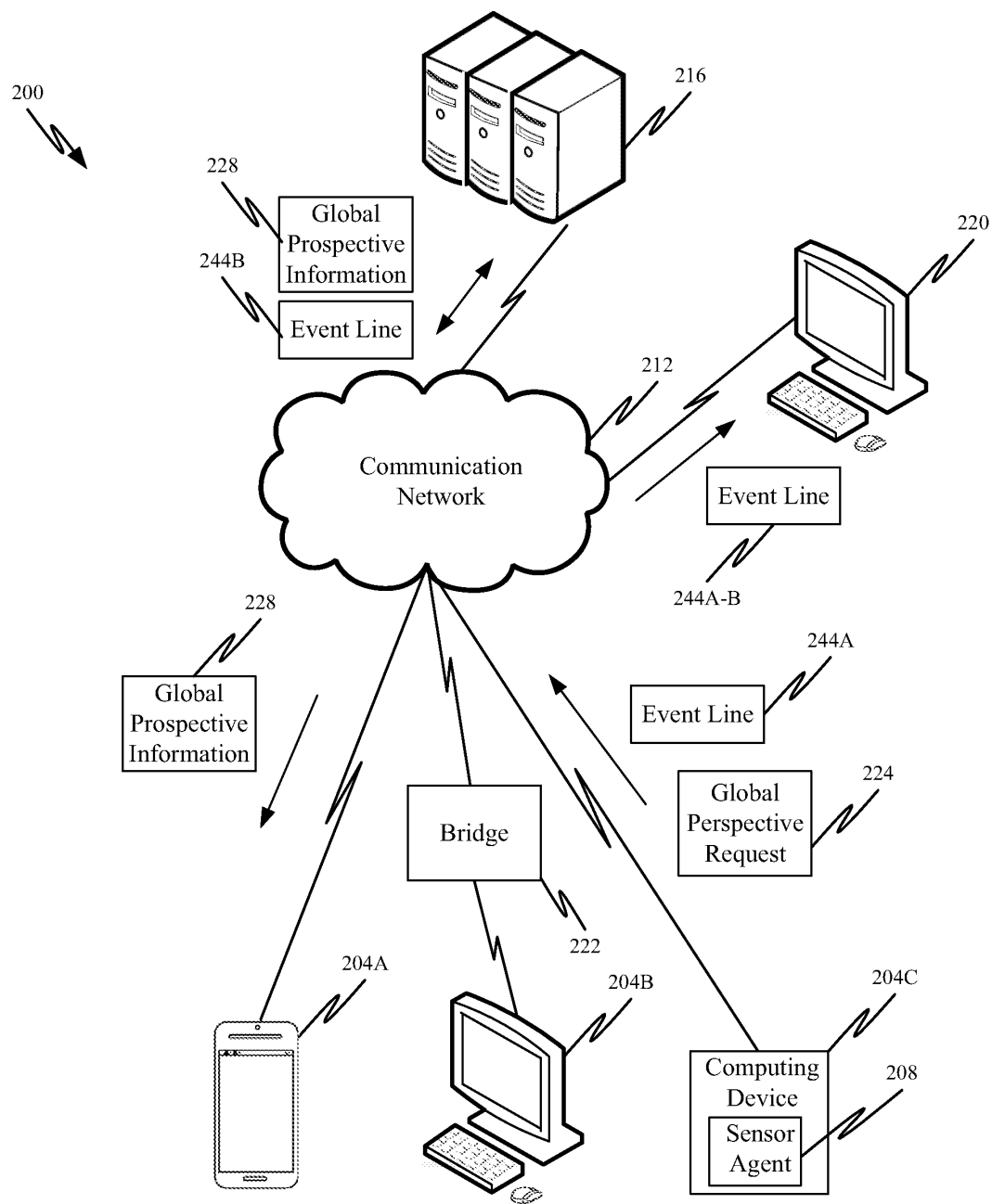


Figure 2

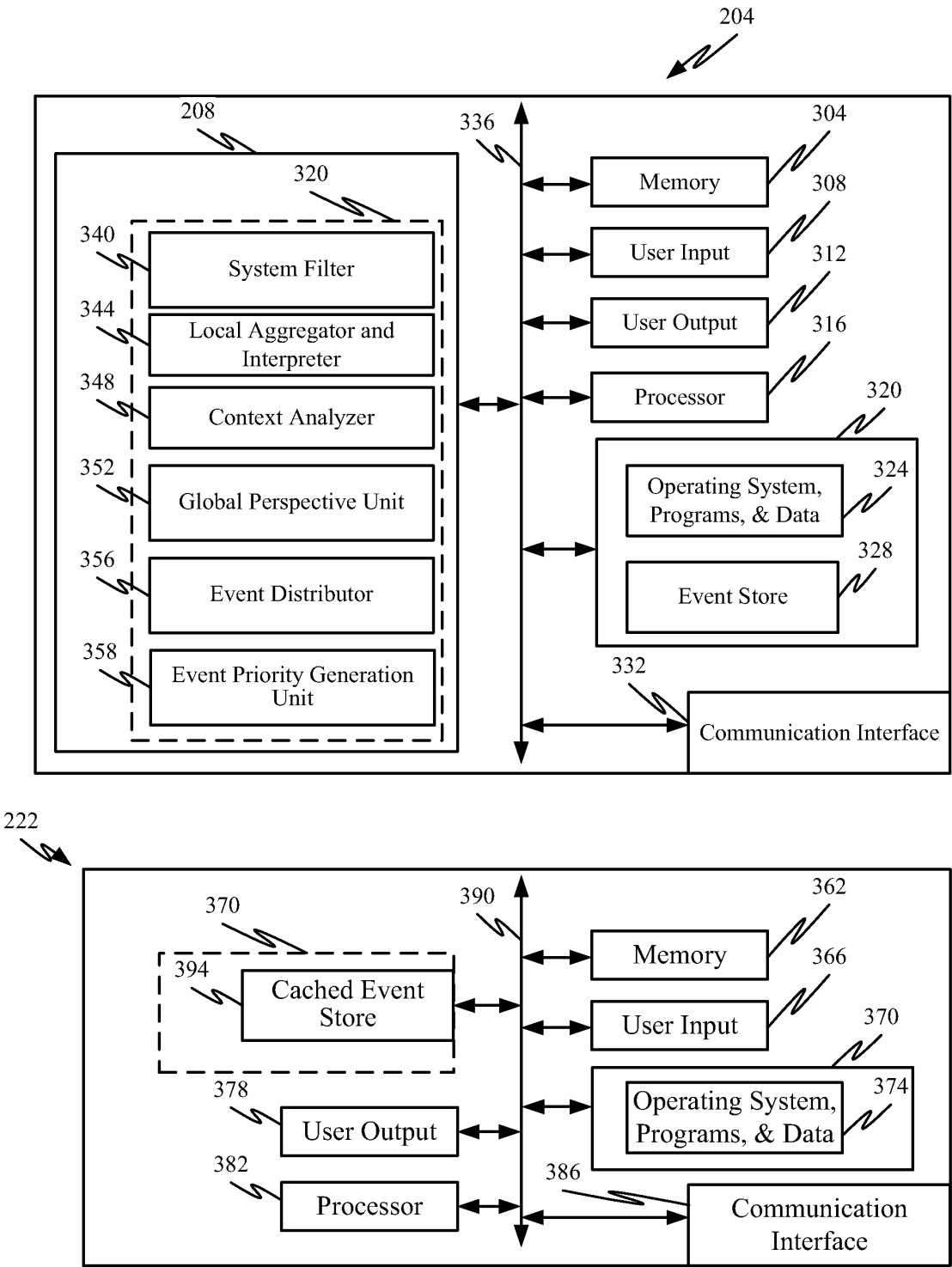


Figure 3

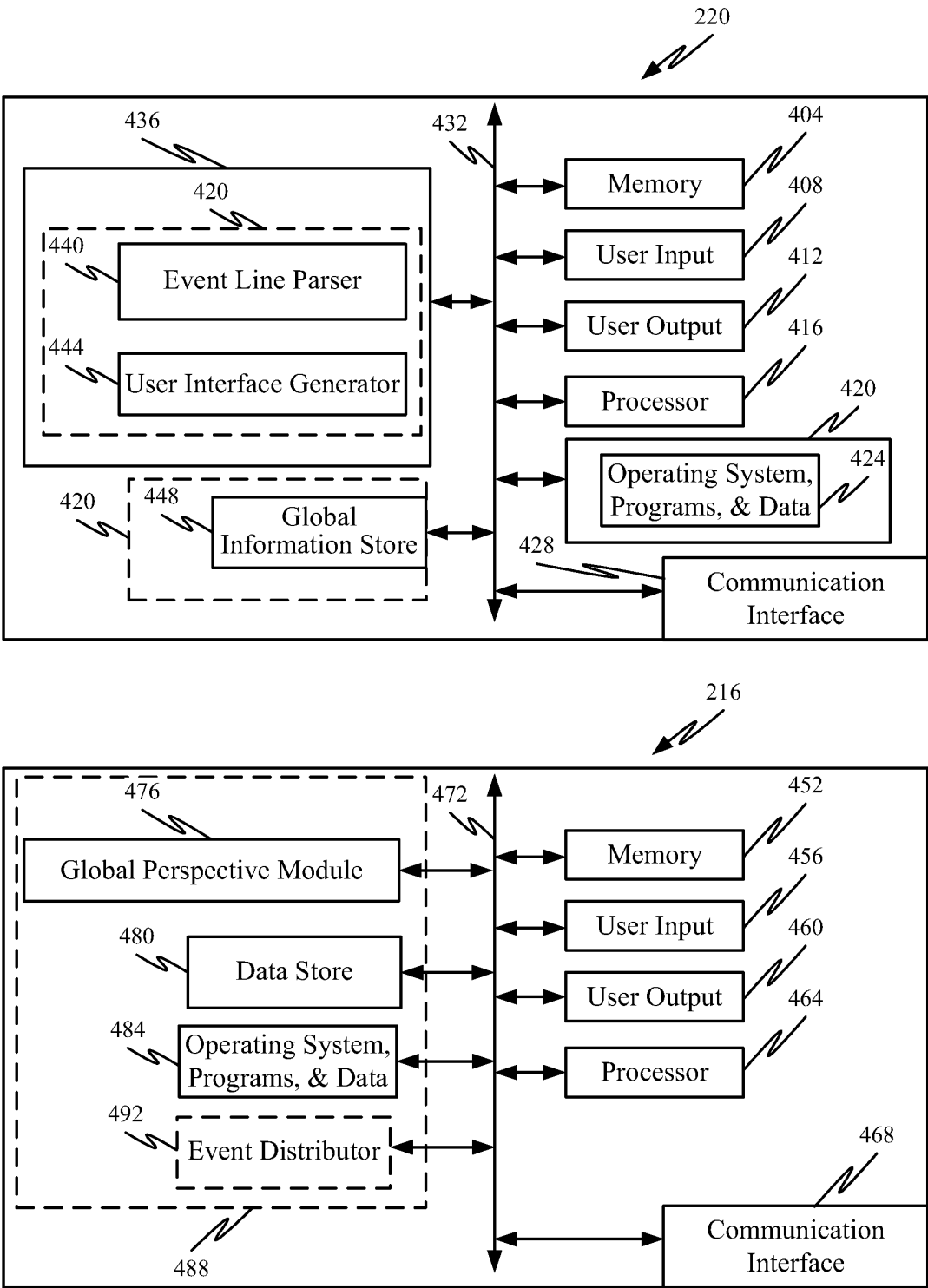


Figure 4

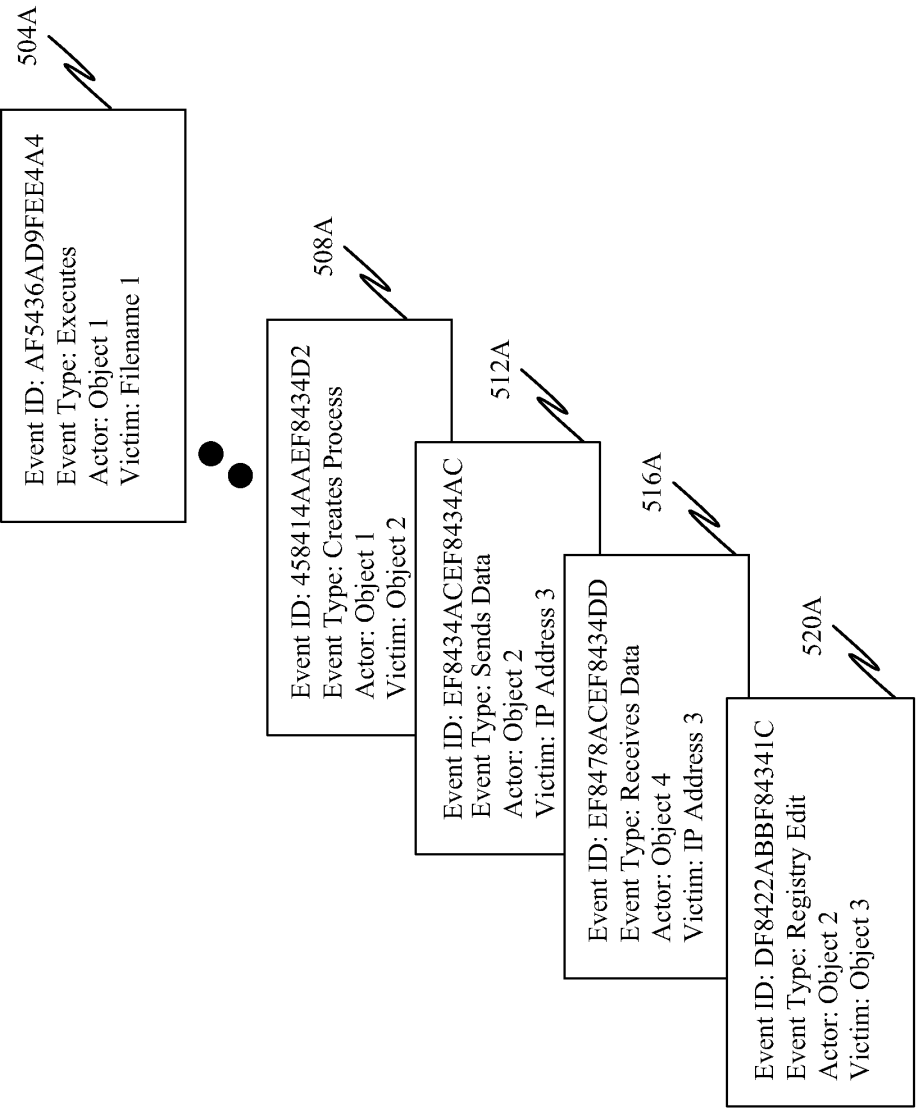


Figure 5A

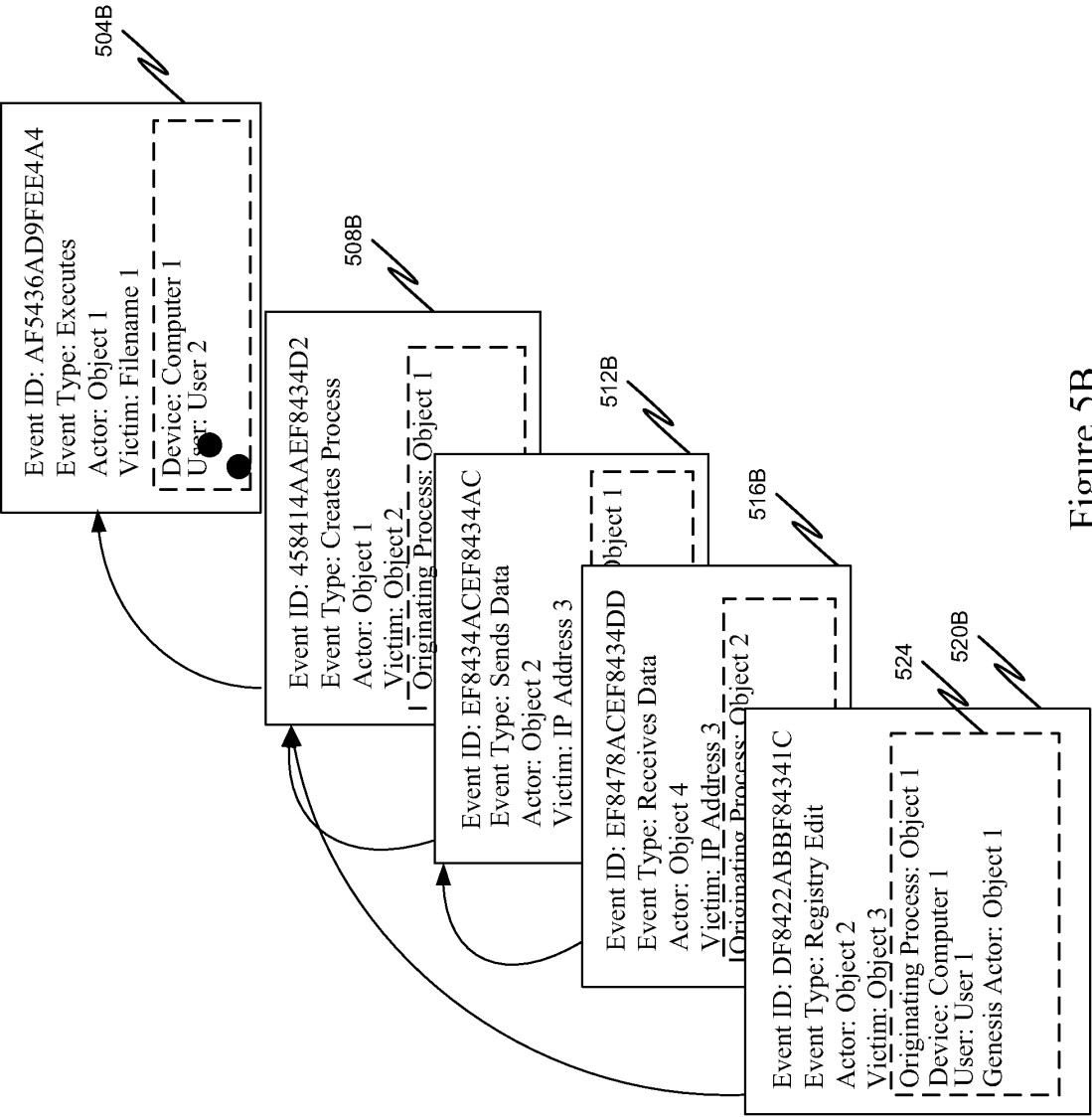


Figure 5B

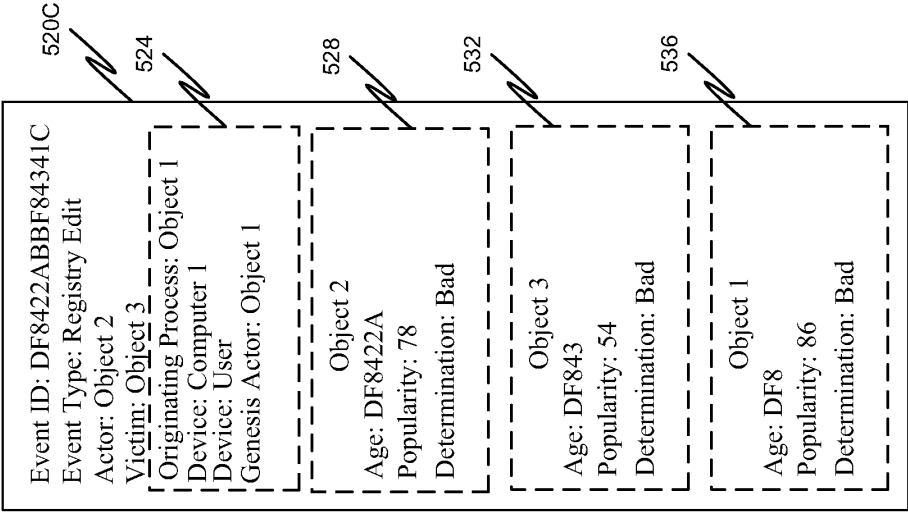


Figure 5C

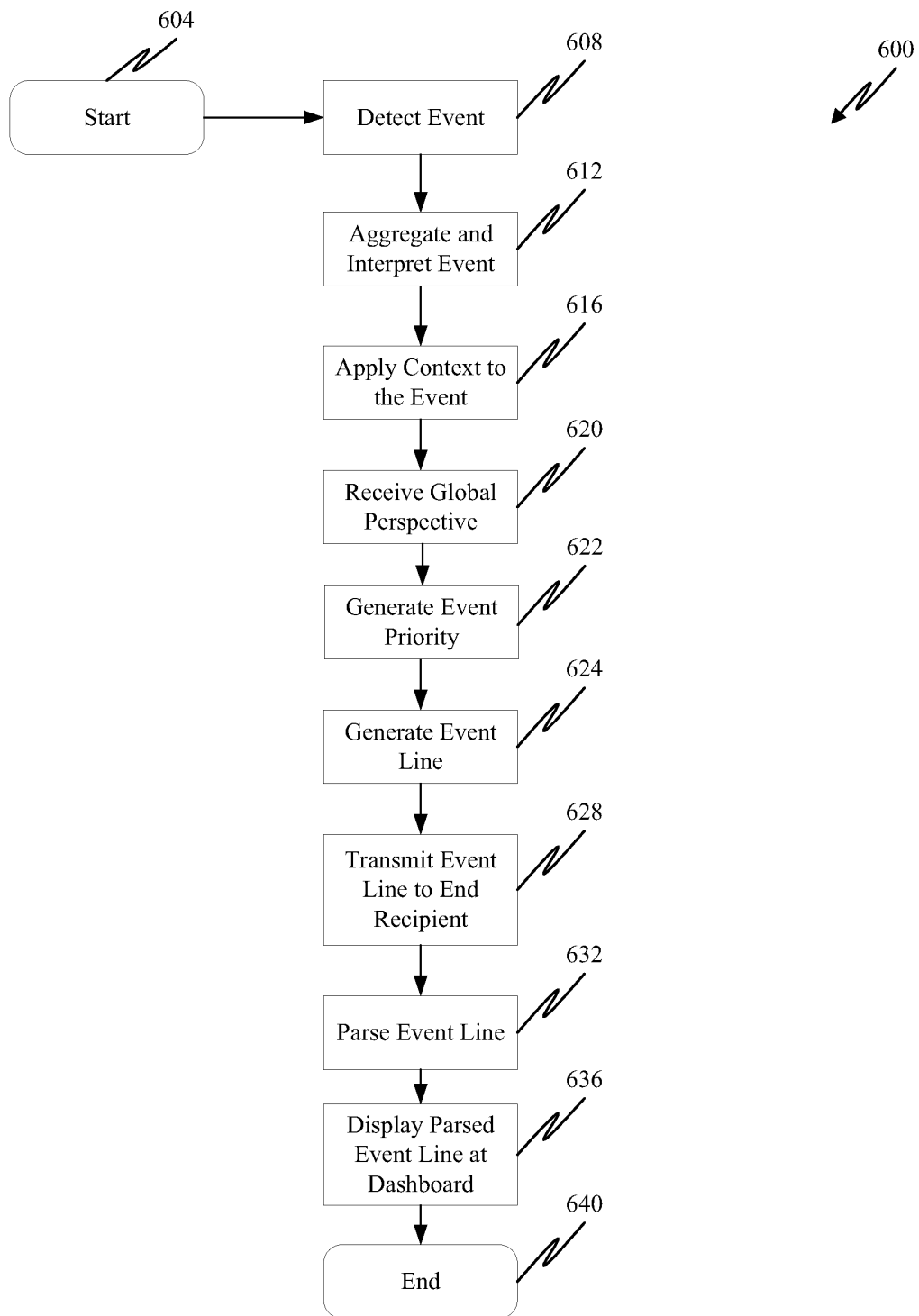


Figure 6

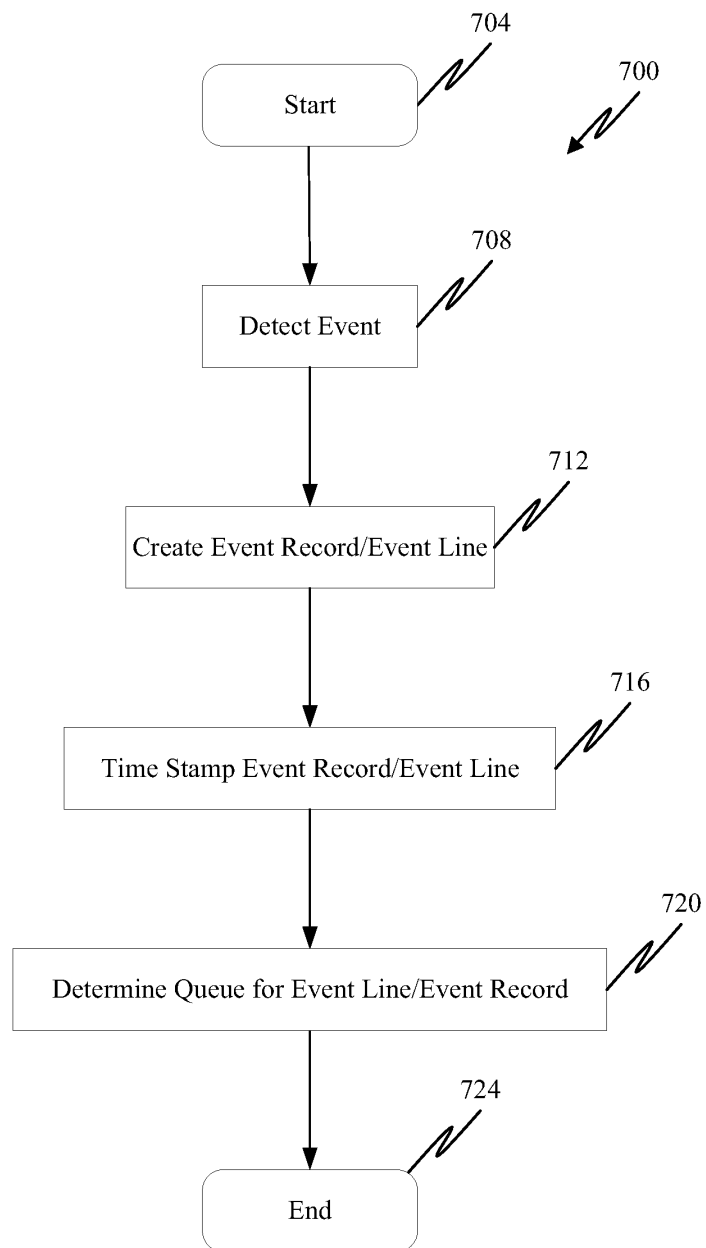


Figure 7

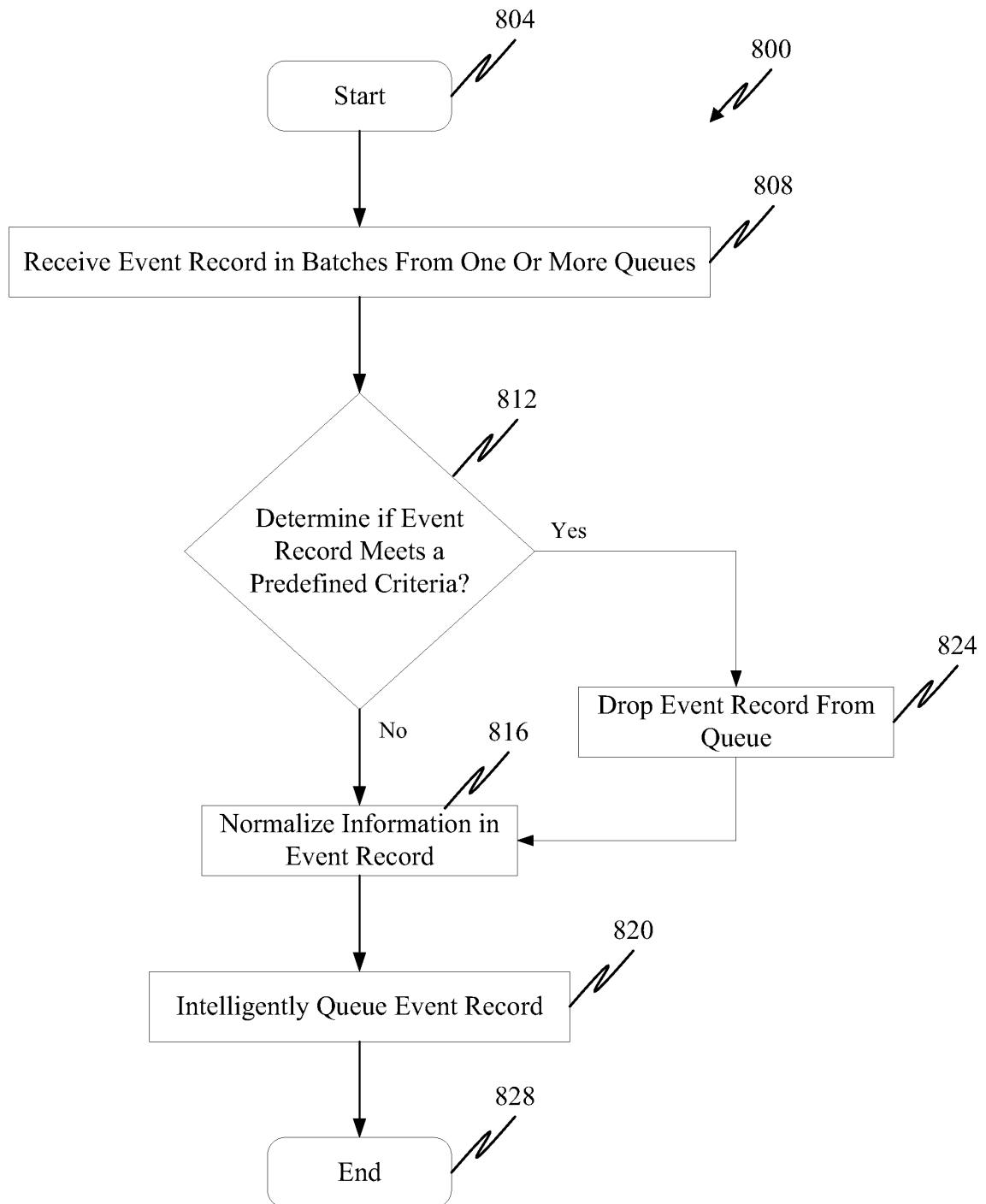


Figure 8

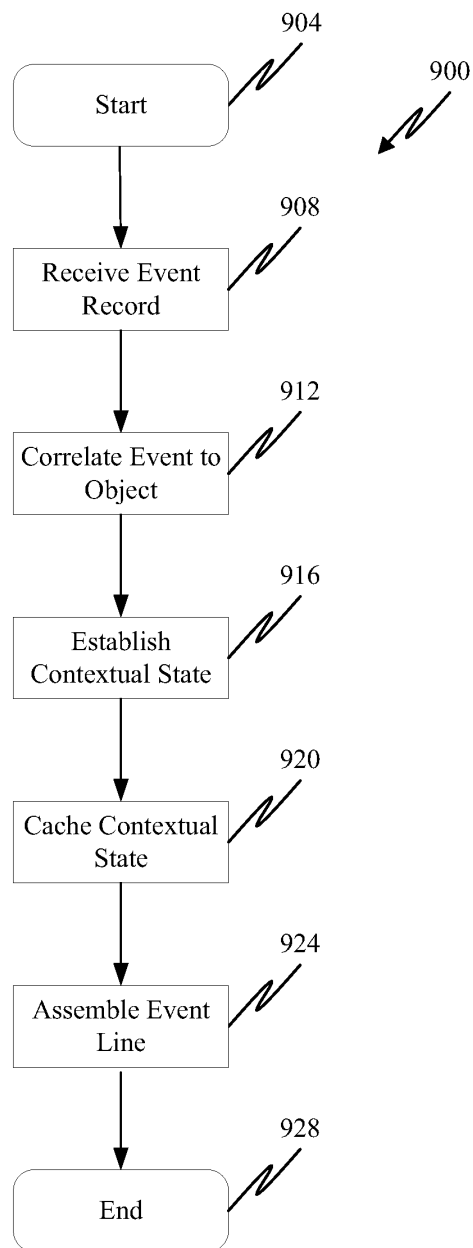


Figure 9

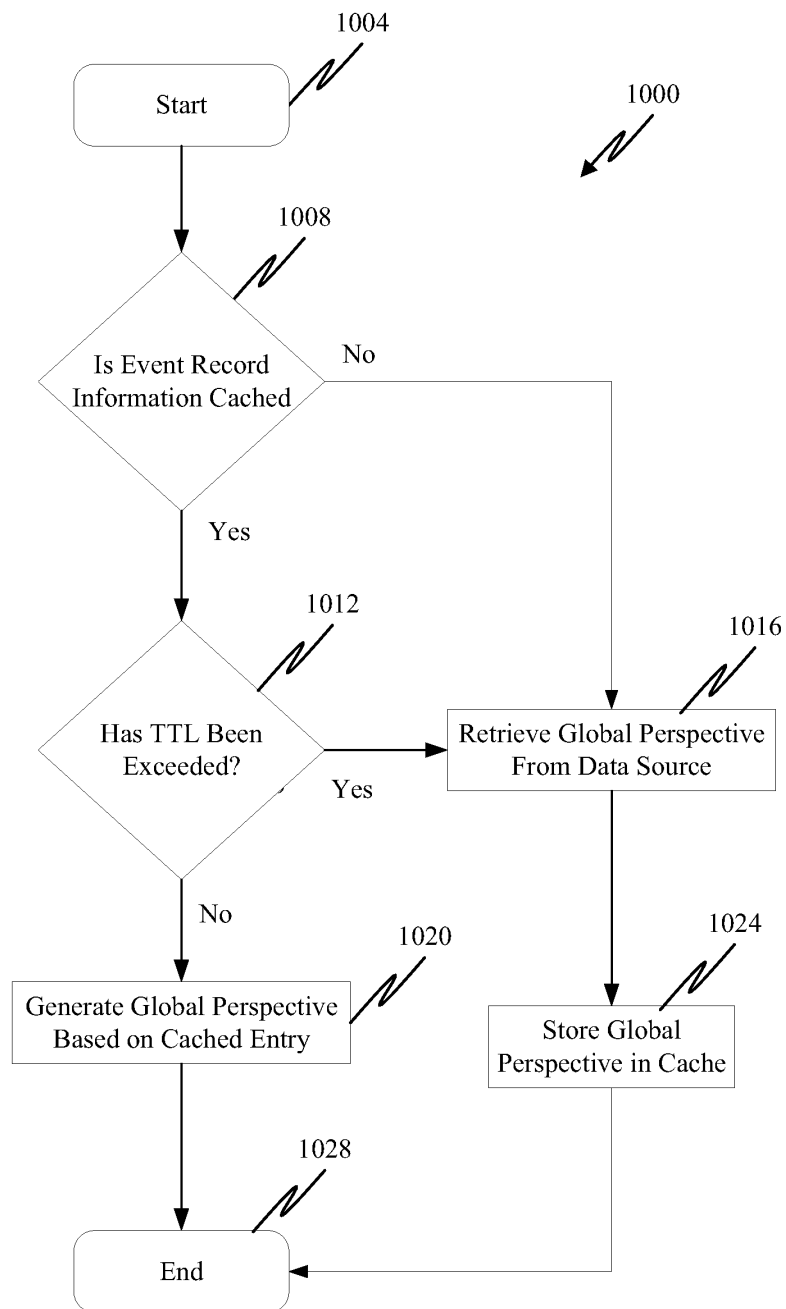


Figure 10

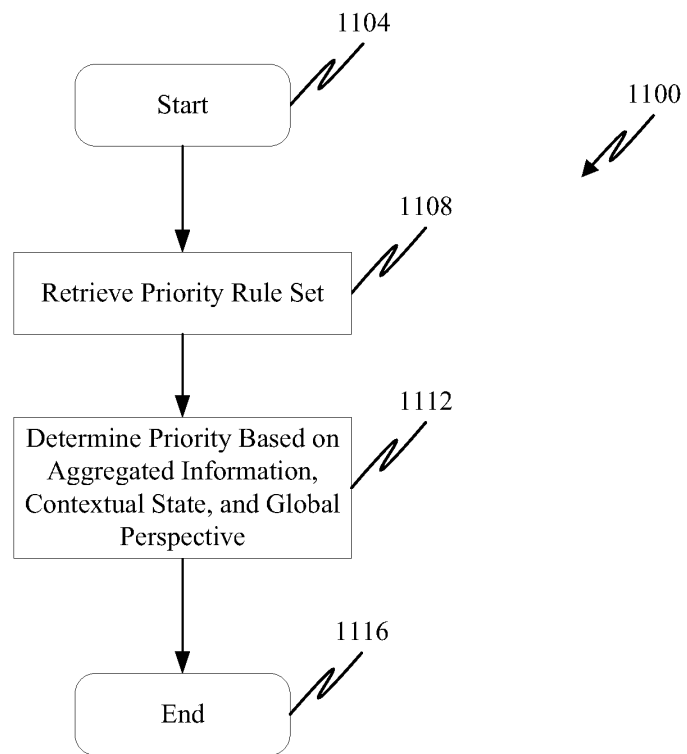


Figure 11

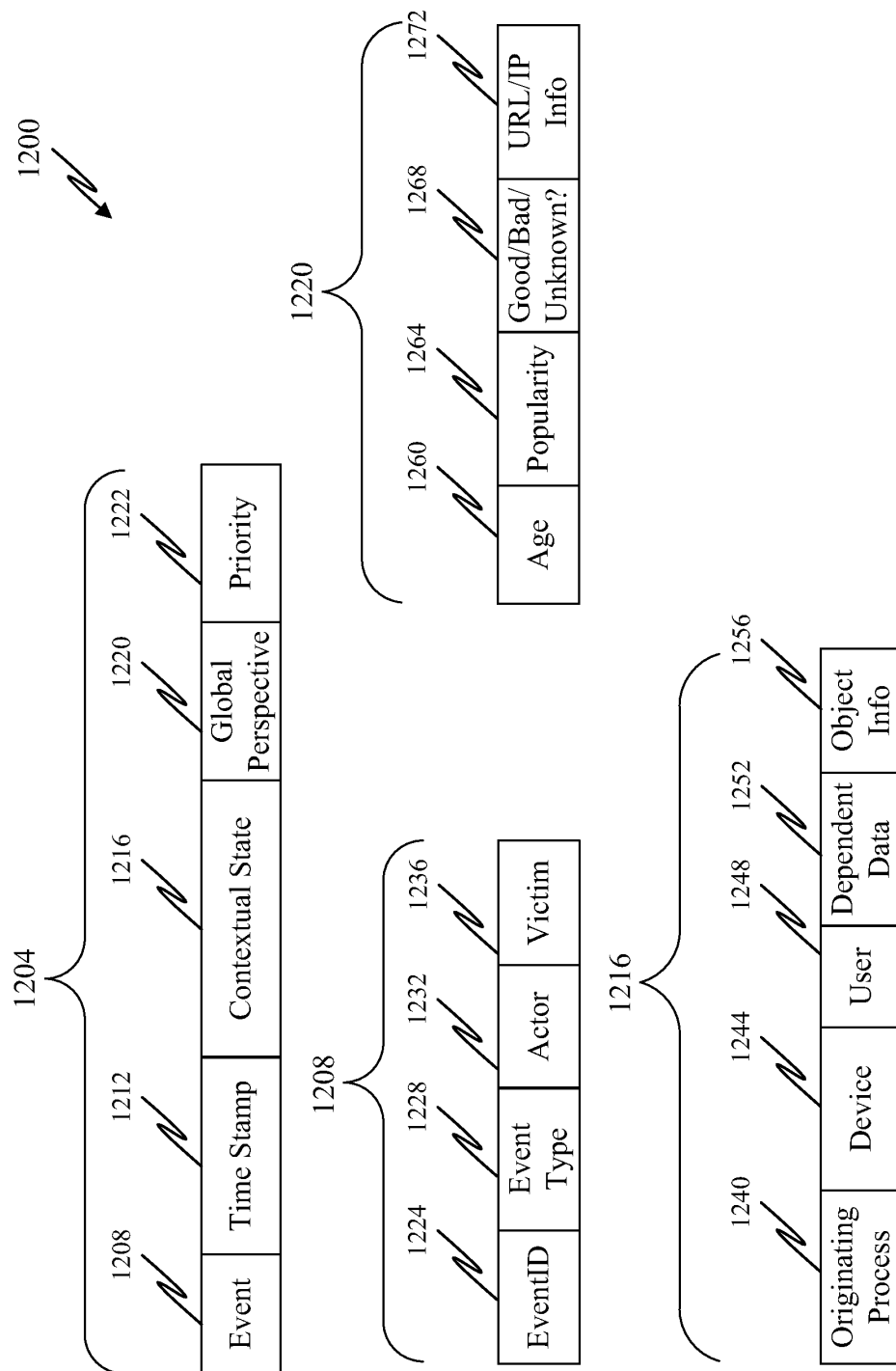


Figure 12

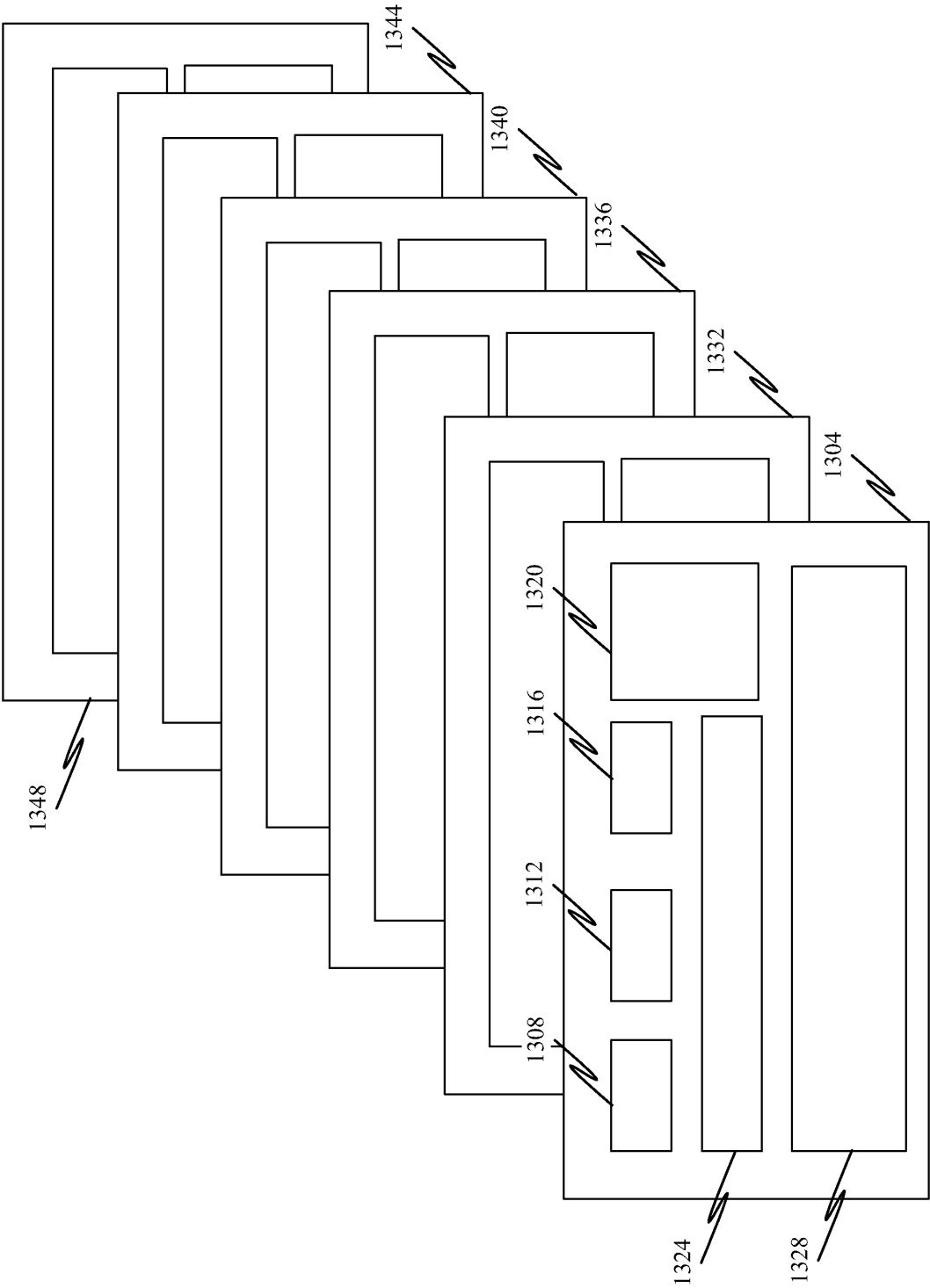


Figure 13