

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

AO KASPERSKY LAB
Petitioner

v.

WEBROOT, INC.
Patent Owner

IPR2023-_____
U.S. Patent No. 10,257,224

**PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT 10,257,224
UNDER 35 U.S.C. § 312 AND 37 C.F.R. § 42.104**

TABLE OF CONTENTS

I. INTRODUCTION	1
II. SUMMARY OF THE '224 PATENT.....	2
A. Description of the '224 Patent.....	2
B. Summary of the Prosecution History	4
C. Claim Construction Under 37 C.F.R. § 42.104(b)(3).....	5
D. Level of Skill of a Person Having Ordinary Skill in the Art.....	6
III. REQUIREMENTS UNDER 37 C.F.R. § 42.104.....	7
A. Grounds for Standing Under 37 C.F.R. § 42.104(a)	7
B. Identification of Challenge Under 37 C.F.R. § 42.104(b).....	7
IV. THERE IS A REASONABLE LIKELIHOOD THAT THE CHALLENGED CLAIMS ARE UNPATENTABLE	8
A. Ground 1: Morris renders Claims 1-2, 4, 8, 10-13, and 17 Obvious.....	8
B. Ground 2: Morris in view of Van Oorschot renders Claims 3 and 17 Obvious	29
C. Ground 3: Capalik renders Claims 1-2, 4, 7-8, 10-13, and 16-19 Obvious	36
D. Ground 4: Capalik in view of Van Oorschot renders Claims 3 and 17 Obvious	67
V. DISCRETIONARY DENIAL IS NOT WARRANTED	70
A. The Advanced Bionics Framework Favors Institution Under § 325(d).....	70
B. The General Plastic Factors Favor Institution	72
C. The Fintiv Factors Favor Institution.....	73
VI. CONCLUSION	78
VII. MANDATORY NOTICES UNDER 37 C.F.R. § 42.8.....	79
A. Real Parties-in-Interest Under 37 C.F.R. § 42.8(b)(1)	79
B. Related Matters Under 37 C.F.R. § 42.8(b)(2).....	79

C. Lead and Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3).....	80
APPENDIX OF EXHIBITS	81
CLAIM LISTING APPENDIX.....	83
CERTIFICATE OF COMPLIANCE UNDER 37 C.F.R. § 42.24(d).....	87
CERTIFICATE OF SERVICE	88

I. INTRODUCTION

AO Kaspersky Lab (“Petitioner”) respectfully requests *inter partes* review (“IPR”) of claims 1-4, 7-8, 10-13, and 16-19 (“Challenged Claims”) of U.S. Patent No. 10,257,224 (“’224 Patent”). Central to the instant challenge is remedying Patent Owner’s attempt to recapture subject matter that was published in its own unrelated patent application nearly eight years before the ’224 Patent’s priority date. Since 2005, Patent Owner has interwoven the concepts at the heart of the Challenged Claims into its various chains of patent applications. The first chain link was a foreign application filed on June 30, 2005. That disclosure ultimately published as U.S. Patent Pub. No. 2007/0016953 to Morris et al. (“*Morris*”)—nearly six years before the provisional application to which the ’224 Patent claims priority. As set forth below in Ground 1, the Challenged Claims improperly seek to recapture the concepts disclosed in 2005 and published in 2007.

Indeed, Patent Owner has acknowledged the connection between its distinct unrelated sets of patent filings. The ’224 Patent incorporates by reference Patent Owner’s U.S. Application Ser. No. 13/372,375, filed Feb. 13, 2012, which itself incorporates by reference the 2007 *Morris* publication for its disclosed methods of dealing with malware. Because the 2007 *Morris* publication was only indirectly incorporated by reference into the ’224 Patent, it was not apparent during prosecution that core principles to which the Challenged Claims are directed were

in fact published many years earlier in an unrelated application.¹ Had the examiner been made aware of these earlier disclosures, the Challenged Claims would not have issued.

II. SUMMARY OF THE '224 PATENT

A. Description of the '224 Patent

Generally directed to systems and methods “for providing forensic visibility” into networks and computer systems, the '224 Patent purports to have improved methods for providing “audit trails” created for threat events occurring within computing devices. '224 Patent (Ex. 1001), 1:17-20, Abstract; *see also id.* at 3:48-52, 8:39-43, 12:65-13:2. While the '224 Patent acknowledges existing network forensic tools, such as network sniffers and packet capturing tools, provide some degree of visibility into network security, these network edge devices receive network events outside of a host or system and therefore “have no ability to establish any sort of context from within the host or system that is generating the event.” *Id.*, 1:42-51. The '224 Patent, therefore, describes techniques “whereby events occurring

¹ *Morris* was cited in an International Search Report attached to a foreign reference provided to the Office during prosecution. Critically, however, *Morris* was only cited as relevant to the claims of this foreign reference (WO 2012/110501) and not the claims of the '224 Patent. *See, e.g., '224 File History* (Ex. 1002), 252.

within a computing device are captured and additional context and a global perspective is provided for each capture event.” *Id.*, 2:25-29. These techniques are recited in the Challenged Claims, including: (1) gathering events defining actions of objects; (2) generating contextual information for the events; (3) obtaining a global perspective for these events; (4) assembling an event line including details associated with the events; and (5) transmitting the assembled event line. *Id.*, 7:14-10:9, Fig. 6.

In (1), “Events” comprise 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’).” *Id.*, 7:34-55. Examples are illustrated below 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

Id., 7:60-8:6. This event data may be represented in the form of a “key” generated by a hashing function to uniquely identify the data. *Id.*, 8:8-14, 17:21-34. In (2), contextual state information is obtained which “may include...originating processes,

devices, and users[,]” or the “GenesisActor,” which is the “ultimate parent of the event being performed.” *Id.*, 8:50-56. In (3), a global perspective is obtained which may include “information related to the age, popularity, and determination of an object of the event—whether it is known good, bad, or unknown.” *Id.*, 9:12-34, Fig. 5C. In (4), an event line is created comprising information relating to the event and in (5), this event line is transmitted. *Id.*, 9:57-10:9.

B. Summary of the Prosecution History

Application No. 15/437,275 (the “’275 Appl.”) which issued as the ’224 Patent claims priority to a provisional application filed on May 3, 2013, which means the first inventor to file provisions of the Leahy-Smith America Invents Act (AIA) apply. For this proceeding, Petitioner applies May 3, 2013, as the priority date for the Challenged Claims.

The ’275 Appl. was filed on February 20, 2017 as a child continuation of U.S. Patent No. 9,578,045. The parent ’045 Patent issued on February 21, 2017, one day after Applicant filed this child application. The originally presented claims of the ’275 Appl. are *identical* to the first claim set Applicant presented during prosecution of the parent ’045 Patent. *Compare ’224 Patent File History*, 17-23 with *’045 Patent File History* (Ex. 1010), 173-179. This common claim set underwent several rejections, including one substantive set of novelty rejections finding all claims obvious over U.S. Publication No. 2013/0298244 to Kumar et al. (“*Kumar*”) in view

of U.S. Publication No. 2008/0016570 to Capalik et al. (“*Capalik ’570*”). ’224 Patent File History, 101-106. *Kumar* was found to teach all limitations of the independent claims apart from assembling an event line and transmitting the assembled event line, which *Capalik ’570* disclosed. *Id.*

Commensurate with the arguments and amendments made in the related ’045 prosecution, Applicant filed an amendment and response, arguing:

Kumar is focused on the integrity of a single application running on a single device. There is simply no teaching of events relating to application integrity for other devices on a network. Therefore, **Kumar cannot possibly teach or suggest a “global perspective” that “relates to one or more other events related to the event across a network.”**

Id., 293-294.² A Notice of Allowance issued thereafter. *Id.*, 296.

As explained in the Grounds below, *Morris*, *Capalik*, and *Van Oorschot* expressly disclose the allegedly patentable community-based anti-malware methods which compare event data across a network to determine a global perspective for an event. *Infra*.

C. Claim Construction Under 37 C.F.R. § 42.104(b)(3)

In this proceeding, claims are interpreted under the same standard applied by

² All emphasis added by Petitioner unless noted otherwise.

Article III courts (i.e., the *Phillips* standard). 37 C.F.R. § 42.100(b); *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (*en banc*). Petitioner applies the ordinary and customary meaning of the claim terms as understood by a PHOSITA for all terms.³

D. Level of Skill of a Person Having Ordinary Skill in the Art

As of May 3, 2013, a person having ordinary skill in the art (PHOSITA) would be a person having a bachelor’s degree in computer science, computer engineering, or an equivalent, as well as two years of industry experience and would have had a working knowledge of host monitoring systems, software security analysis, and dynamic malware analysis. Additional graduate education could substitute for professional experience, or significant experience in the field could substitute for formal education. Dr. Lee Declaration (“*Decl.*”) (Ex. 1003), ¶¶ 32-35.

³ Petitioner’s challenge is not a waiver of any argument in litigation that any claim term in the ’224 Patent is indefinite or invalid. And Petitioner does not waive its rights to seek to construe claim terms in litigation, including in the pending district-court litigation.

III. REQUIREMENTS UNDER 37 C.F.R. § 42.104

A. Grounds for Standing Under 37 C.F.R. § 42.104(a)

Petitioner certifies the '224 Patent is eligible for IPR.

B. Identification of Challenge Under 37 C.F.R. § 42.104(b)

Petitioner requests the Challenged Claims be found unpatentable on the following grounds:

Proposed Ground of Unpatentability	Exhibits
<u>Ground 1:</u> Claims 1-2, 4, 8, 10-13, and 17 are obvious under § 103(a) over U.S. Publication No. 2007/0016953 to Morris et al. (“ <i>Morris</i> ”)	Ex. 1005
<u>Ground 2:</u> Claims 3 and 17 are obvious under § 103(a) over <i>Morris</i> in view of U.S. Patent No. 8,087,087 to Van Oorschot et al. (“ <i>Van Oorschot</i> ”)	Ex. 1005, Ex. 1006
<u>Ground 3:</u> Claims 1-2, 4, 7-8, 10-13, and 16-19 are obvious under § 103(a) over U.S. Publication No. 2011/0321166 to Capalik et al. (“ <i>Capalik</i> ”)	Ex. 1008
<u>Ground 4:</u> Claims 3 and 17 are obvious under § 103(a) over <i>Capalik</i> in view of <i>Van Oorschot</i>	Ex. 1008, Ex. 1006

This Petition, supported by the declaration of V.S. Subrahmanian, Ph.D.⁴ (“Subrahmanian Decl.” (Ex. 1031)), demonstrates that there is a reasonable likelihood that Petitioners will prevail with respect to cancellation of at least one challenged claim. See 35 U.S.C. § 314(a).

IV. THERE IS A REASONABLE LIKELIHOOD THAT THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. Ground 1: Morris renders Claims 1-2, 4, 8, 10-13, and 17 Obvious

Overview of Morris

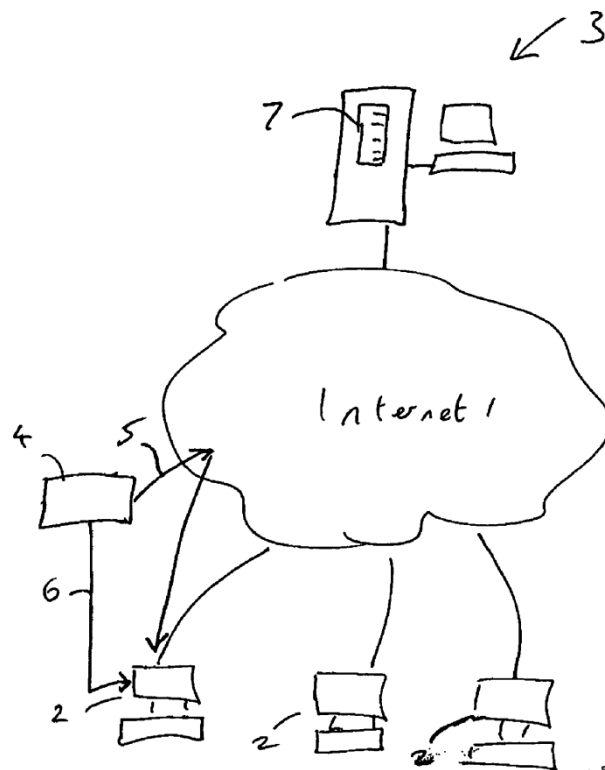
Morris was filed on June 30, 2006 and published on January 18, 2007 and therefore qualifies as prior art to the '224 Patent under 35 U.S.C. §§ 102(a)(1) and 102(a)(2). *Morris* (Ex. 1005). *Morris* was not cited or considered during prosecution of the '224 Patent.

Morris discloses community-based methods “of classifying a computer object as malware,” comprising “receiving data about a computer object from each of plural

⁴ Kaspersky has retained V.S. Subrahmanian, Ph.D. in this proceeding. See Ex. 1031. V.S. Subrahmanian has adopted the opinions set forth in Ex. 1003, the declaration of Dr. Lee, as his own. Ex. 1031, ¶ 12. While Kaspersky is not relying directly on Dr. Lee’s declaration in this Petition, for expediency this Petition cites only to Ex. 1003.

remote computers on which the object or similar objects are stored; comparing in the base computer the data about the computer object received from the plural computers; and, classifying the computer object as malware on the basis of said comparison.” *Morris*, [0014]-[0016], Abstract. These methods “may be carried out by so-called agent software running on the remote computer.” *Id.*, [0033].

Figure 1 below depicts an apparatus for accomplishing *Morris*’s methods:



Id., Fig. 1. In Figure 1, computing devices 202 (e.g., personal computer, server, PDA, mobile phone) are connected to “‘base’ computer 3” over network 1. *Id.*, [0077]. Computing devices 202 run an object 4, and if the object is unknown locally,

“local ‘agent’ software” running on each device sends information relating to the object and its effects to base computer 3. *Id.*, [0077]-[0079], [0086]. This information may include the same event data disclosed in the ’224 Patent:

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

Id., [0105]. Additional contextual information can be sent to base computer 3, such as the “‘Genesisactor’—the key of an object that is not the direct Actor of an event but which is the ultimate parent of the event being performed.” *Id.*, [0107]. This contextual “allow[s] ancestral relationships to be considered for any object and its predecessors[.]” *Id.*, [0099]; *see also id.* at [0052]. The base computer analyzes this information and determines whether the object is safe or unsafe (i.e., malware). *Id.*, [0096]-[0103], [0110].

Because *Morris*, like the ’224 Patent, discloses methods for providing computer security by analyzing event data from potential threat events, *Morris* is in the same field of endeavor as the ’224 Patent. *Compare Morris*, [0001], [0014]-[0017] with ’224 Patent, 4:45-65, 9:52-56; *Decl.*, ¶¶ 54-62. *Morris* is also directed at solving similar problems faced by the inventors of the ’224 Patent, such as analyzing ancestral or audit information to make a malware determination. *Compare*

Morris, [0052], [0099], [0128]-[0135] with '224 Patent, 3:48-61, 8:29-49, 12:58-66, 18:60-65; *Decl.*, ¶¶ 54-62.

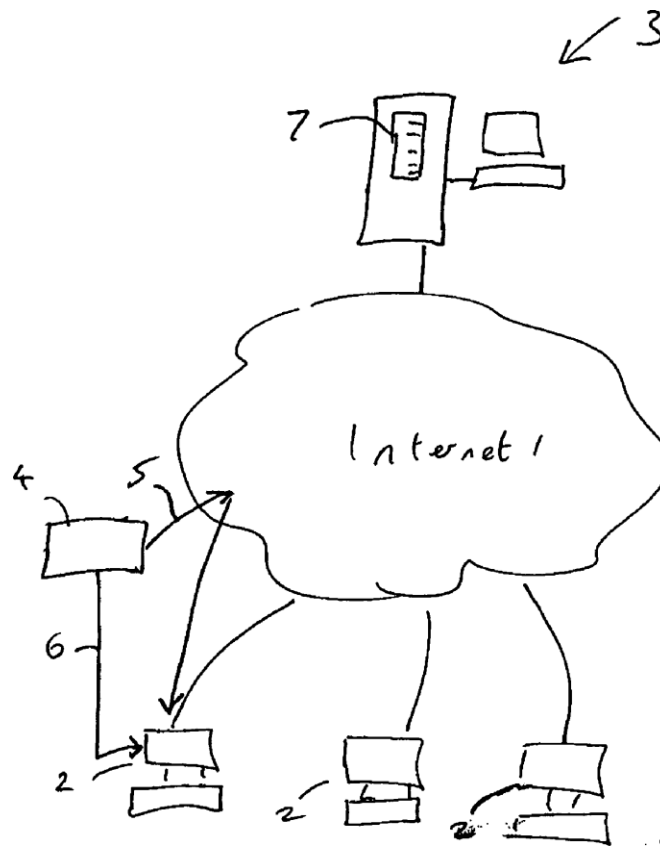
1. Claim 1

1[P]. A method comprising:

To the extent the preamble is found limiting, *Morris* discloses “**methods** and apparatus for dealing with malware.” *Morris*, [0001] (disclosing a “**method** and apparatus for classifying a computer object as malware”). This method may comprise “at a base computer, receiving data about a computer object from each of plural remote computers on which the object or similar objects are stored; comparing in the base computer the data about the computer object received from the plural computers; and, classifying the computer object as malware on the basis of said comparison.” *Id.*, [0014]-[0016].

[1(a)] gathering an event defining an action of a first object acting on a target,

Morris discloses that “the base computer” gathers “**events initiated by or involving the object when the object is created, configured or runs on the respective remote computers.**” *Morris*, [0018]. Figure 1 depicts the components involved in *Morris*’s disclosed methods:



Id., Fig. 1. Remote computers 2 “run an object 4” and gather and transmit “information relating to each object run on all of the connected remote computers” to community database 7. *Id.*, [0078]. The “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.” *Id.*, [0081]. This information is passed in “the form of a so-called signature or key relating to the object and its effects.” *Id.*, [0078], [0086].

This key may include several components, including “components representing data about said object” such as “events.” *Id.*, [0087], [0105].

“‘Events’...define the actions or behaviours of an object acting upon another object or some other entity.” *Id.* An “event has three principal components: the key of the object performing the act (the ‘**Actor**’), the act being performed (the ‘**Event Type**’), and the key of the object or identity of another entity upon which the act is being performed (the ‘**Victim**’).” *Id.* Examples of the three components of an event are shown below:

First Object	Action	Target
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

Id. (annotated); *see also id.*, [0107] (describing “software installation” event). *Morris*’s disclosure of gathering the event data depicted in the table above is nearly identical to the ’224 Patent’s disclosure. *See, e.g.,* ’224 Patent, 7:61-8:6 (disclosing **identical** table of event information); *Decl.*, ¶¶ 77-81. *Morris* therefore discloses *gathering an event defining an action of a first object acting on a target* in the same way described in the ’224 Patent.

[1(a)(i)] wherein the first object is executed on a device;

Morris discloses *the first object is executed on a device*. *Supra*, Claim [1(a)] (remote computer “run[s] an object”).

[1(b)] generating contextual state information for the event by correlating the event to an originating object of the first object;

Morris discloses that additional contextual data correlated to the event is captured, including the “**Genesisactor**” (i.e., *originating object of the first object*) which is the “object that is not the direct Actor of an event but which is **the ultimate parent of the event being performed.**” *Morris*, [0058], [0107]. Example event two is highlighted below:

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

Morris, [0105] (annotated). The “Genesisactor” generated from this event would be the “ultimate parent of the event being performed”—such as the executable file that created “Object 1” (i.e., the *first object*). *Decl.*, ¶¶ 83-86. By correlating event two with the “Genesisactor” responsible for creating Object 1, *Morris* teaches generating contextual state information for the event by *correlating the event to the originating object of the first object*. *Id.*

Morris’s disclosure of correlating “Genesisactor” data with an event is consistent with the ’224 Patent’s disclosure of *generating contextual state information*. The ’224 Patent explains that:

“contextual state information may include GenesisActor information...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.”

'224 Patent, 8:50-56. Compare *id.*, 17:35-40 (“a contextual analysis may be applied to the captured events 504B-520B. Accordingly, a context 520B comprising an origination process [sic], Device, User, and in some instances, a GenesisActor may further supplement or enhance the Event ID, Event Type, Actor, and Victim”) with *Morris*, [0099] (“For example, analysis can be made of which object created this object, which objects this object created...In this regard an object is considered to have a relationship based on the event performed by it upon another object, or upon it by another object. This simple 1-to-1 relationship chain...”).

Therefore, *Morris* discloses *generating contextual state information for the event by correlating the event to an originating object* in the same way described in the '224 Patent.

[1(c)] obtaining a global perspective for the event based on the contextual state information,

Morris discloses that after event data and associated contextual metadata (e.g., Genesisactor) is gathered and generated, this data is then sent to base computer 3. *Morris*, [0014]-[0017], [0020], [0078]. Base computer 3 compares “the data about the computer object received from the plural computers” and “**classif[ies] the**

computer object as malware on the basis of said comparison.” *Id.*, [0016], [0017] (“this aspect allows a comparison to be made between the objects and/or their effects on the different remote computers to determine whether or not a particular object should be classed as good or as malware”), [0081]-[0084] (describing process for determining object is “bad or unsafe”). This comparison involves identifying “relationships between the object and other objects” to “immediately and automatically [] **mark a child object as bad** (or good) [] **or a parent or other related object [a]s bad** (or good).” *Id.*, [0019], [0096]; *see also id.*, [0096]-[0103] (describing heuristics run on the event data in database 7, including a heuristic for analyzing “an object’s relationship to other objects that act upon it or upon which it acts” “for the rapid identification and **determination of malware**” for a child, parent, or other related object), [0128]-[0134].

Morris’s disclosure of obtaining a global perspective by determining whether a first or originating object is malware based on familial relationships is consistent with the ’224 Patent’s disclosure of *obtaining a global perspective for the event based on the contextual information*. The ’224 Patent explains that “obtaining a global perspective for the at least one event” includes “obtaining information associated with one or more of the first object and the originating object” such as “a determination as to whether the first object is malware” and “a determination as to whether the originating object is malware.” ’224 Patent, 4:45-59, 5:11-16, 9:26-28,

17:56-66; *see also id.*, claim 8 (claiming global perspective comprising a malware determination for the first and/or originating objects).

Morris therefore discloses *obtaining a global perspective for the event based on the contextual state information* in the same way described in the '224 Patent.

[1(c)(i)] wherein the global perspective comprises information associated with one or more of 5 the first object and the originating object,

As described above, *Morris* discloses the global perspective comprises information associated with one or more of the first object and the originating object—namely, a determination as to whether the first and/or the originating objects are malware. *Supra*, [1(c)].

[1(c)(ii)] and wherein the global perspective relates to one or more other events related to the event across a network;

Morris discloses that “a preferred embodiment . . . comprises connecting the computer to a community database that is connectable to a plurality of computers, and **uploading the stored data to the community database for comparison with similar data provided by other computers.**” *Morris*, [0067], [0014]-[0016]

⁵ This limitation recites a disjunctive list of alternatives such that Petitioner need only show the prior art discloses one of the recited options of the Markush group to render it unpatentable. *See, Fresenius USA, Inc. v. Baxter Intern., Inc.*, 582 F.3d 1288, 1298 (Fed. Cir. 2009).

(describing running an object on a plurality of remote computers and sending that information to a base computer holding a community database for analysis). “[T]his aspect allows a comparison to be made between the objects and/or their effects on the different remote computers **to determine whether or not a particular object should be classed as good or as malware.**” *Id.*, [0017]; *see also id.*, Fig. 1 (depicting the plurality of remote computers 2 running an object 4 to send data to base computer 3), [0019] (disclosing performing a comparison between the object and “other objects includ[ing] the object or similar objects **stored on at least some of the remote computers**”), [0078] (“The community database 7 is populated, over time, with information relating to each object run on all of the connected remote computers 2”), [0081]. *Morris* therefore discloses obtaining a global perspective for the event that *relates to other related events across the network*, such that a malware determination for the first and/or originating object takes into account related events on other devices. *Id.*, [0017]; *Decl.*, ¶¶ 97-98.

[1(d)] generating an event line comprising information relating to the event,

Morris discloses that its system gathers event data to be “sent from the plural remote computers to the base computer” for subsequent analysis. *Supra*, [1(a)]; *Morris*, [0018]. Remote computers 2 “run an object 4” and gather and transmit “information relating to each object run on all of the connected remote computers” to community database 7. *Id.*, [0078], Fig. 1. This information is passed in “the form

of a so-called signature or key relating to the object and its effects.” *Id.*, [0078], [0086]. Like the ’224 Patent, this key is “formed by a hashing function operating on the object at the remote computer 2.” *Compare id. with* ’224 Patent, 8:12-14.

[1(d)(i)] wherein the information relates to at least one of 6 the first object, the action of the first object, the target, and the originating object; and

This key may include information such as “the key of the object performing the act (the ‘**Actor**’), the act being performed (the ‘**Event Type**’), and the key of the object or identity of another entity upon which the act is being performed (the ‘**Victim**’).” *Id.*, [0105]. It also may include the “‘**Genesisactor**.’” *See Morris*, [0107]); *Decl.*, ¶¶ 100-102. Therefore, *Morris* discloses *generating an event line comprising information relating to the event* including information relating to *the first object (Actor) the action of the first object (Event Type) the target (Victim) and the originating object (Genesisactor)*.

[1(e)] transmitting the generated event line.

As discussed above in limitation [1(d)], *Morris* discloses transmitting its key to base computer 3 for processing. *Supra*, [1(d)]. *Morris* also discloses this key can be subsequently “copied to” the local database of a remote computer that first ran the object. *Morris*, [0084].

⁶ This limitation also recites a Markush group. *Supra*, fn. 4.

2. Claim 2

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.

Morris discloses obtaining information associated with the first object and/or originating object, such as a determination that the first and/or originating objects are malware. *Supra*, [1(c)].

Morris further discloses these malware determinations may be obtained from a community database. *See, e.g., Morris*, [0097]-[0101]; *see also id.*, [0067], [0078]. For example, *Morris* discloses five heuristics which are “run on the data in the **community database 7**” to “establish if an object is safe, unsafe or suspicious.” *Id.*, [0095], [0097], [0110]. Regarding malware determinations, the second heuristic analyzes object relationships stored in community database 7 to make a malware determination. *Id.*, [0100] (“centralisation of the community data in the community database 7 provides the ability to rapidly assimilate object behaviours, allowing for the rapid identification and determination of malware”). Therefore, *Morris* discloses the *information associated with the one or more of the first object and the originating object is obtained from a community database*.

Morris additionally discloses its *event line* is transmitted to base computer 3 (i.e., *end recipient*) for processing, as was well known in the art. *Supra*, Claim [1(d)]; *Decl.*, ¶¶ 103, 105-108. Alternatively, *Morris* discloses its key can be “copied to the

local database of the remote computer 2 that first ran the object[.]” *Morris*, [0084].

A PHOSITA would have understood remote computer 2 would constitute an *end recipient* here. *Decl.*, ¶ 108.

3. Claim 4

4. The method of claim 1, wherein the event includes information identifying the first object performing the action, information identifying the action being performed, and information identifying the target upon which the act is being performed.

As described above, *Morris* discloses “Event” information which includes “three principal components: the key of the object performing the act (the ‘**Actor**’), the act being performed (the ‘**Event Type**’), and the key of the object or identity of another entity upon which the act is being performed (the ‘**Victim**’).” *Supra*, Claim [1(a)].

4. Claim 8

8. The method of claim 1, wherein the global perspective comprises information comprises at least one of 7: an age; a popularity; a determination as to whether the first object is malware; a determination as to whether the originating object is malware; an Internet Protocol (IP) Address; and a Uniform Resource Locator (URL).

Morris discloses obtaining a global perspective comprising a determination as to whether the first and/or originating objects are malware. *Supra*, Claim [1(c)] (describing obtaining this information in the same way as the ’224 Patent).

⁷ This limitation recites a Markush group. *Supra*, Fn. 4.

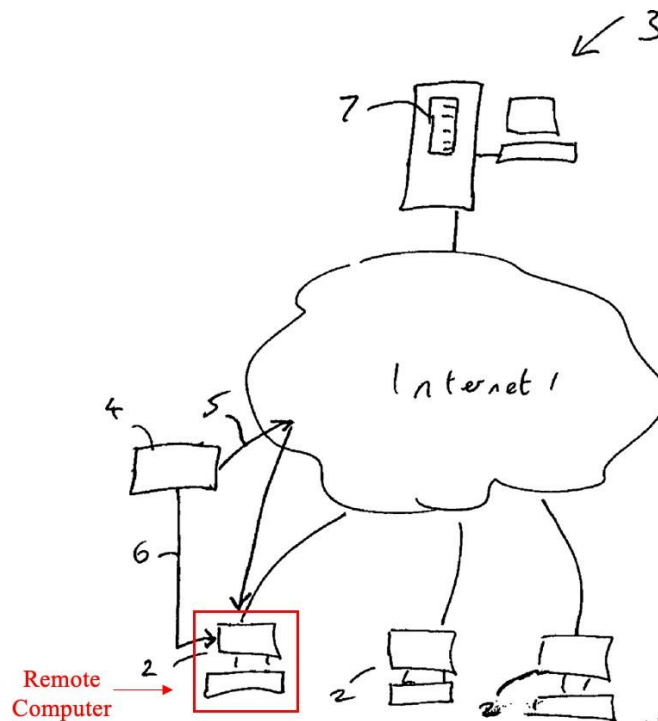
5. Claim 10

10[P] A system for providing forensic visibility into a system, comprising:

To the extent the preamble is found limiting, *Morris* discloses an “apparatus for dealing with malware.” *Morris*, [0001], Fig. 1. Like the ’224 Patent, *Morris*’s system provides forensic visibility into a system by analyzing audit trails or “relationship chain[s]” for events. Compare *Morris*, [0052], [0099] (“relationship chain provides a complex series of correlation points, allowing ancestral relationships to be considered for any object and its predecessors”), [0128]-[0135] with ’224 Patent, 1:18-20 (“systems for providing forensic visibility into client systems having full audit trails are described”).

[10(a)] a device comprising:

Morris discloses its apparatus includes a “**remote computer**” (*device*) used to gather event information to send to a base computer for analysis. *Morris*, [0014]-[0016], [0077]-[0078]. This remote computer is depicted below in Figure 1:



Id., Fig. 1 (annotated, identifying one of several remote computers 2 for simplicity).

[10(b)] a communication interface;

Remote computer 2 is connected to the “**Internet 1**” to enable communication with base computer 3. *Morris*, [0077]. A PHOSITA would have understood this to teach a *communication interface*. *Decl.*, ¶ 114.

[10(c)] a processor;

Morris’s remote computer 2 (e.g., personal computer) is configured to run “local ‘agent’ software” for effectuating the functions therein and therefore includes a processor for executing the functions of this software. *Id.*, [0079]; *see also id.*, [0033], [0065]; *Decl.*, ¶ 115.

[10(d)] data storage; and

Morris discloses its' methods are effectuated by “agent software **running on the remote computer.**” *Id.*, [0033], [0079], [0122] (“computer 2 may have agent software installed...”). A PHOSITA would have understood remote computer 2 therefore includes *data storage* which stores local agent software. *Decl.*, ¶ 116.

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

Supra, [10(c)-(d)] (describing remote computer 2 configured with “local ‘agent’ software” for effectuating the described methods and the processor for executing the functions of the “local ‘agent’ software”).

The remaining limitations of Claim 10 are substantively identical to method steps of Claim 1 and are rendered obvious for the same reasons detailed in Claim 1. *See* Claim Appendix.

6. Claim 11

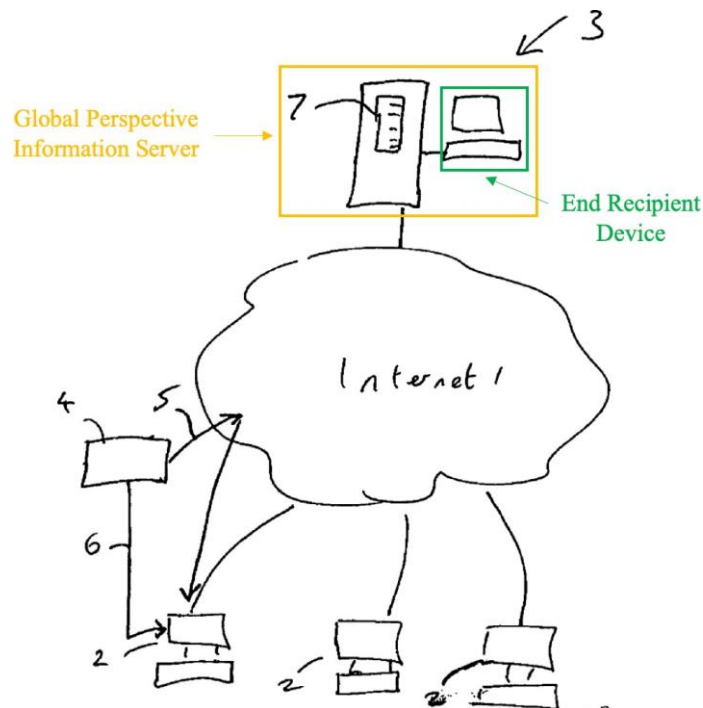
11. The system of claim 10, wherein the event is executed by the processor.

Morris renders the system of claim 10 obvious. *Supra*, claim 10. A PHOSITA would have understood *Morris*’s processor on the remote computer would execute the events described in *Morris*. *Decl.*, ¶ 119.

7. Claim 12

12 The system of claim 10, further comprising: a global perspective information server; and an end recipient device, wherein the information associated with the one or more of the first object and the originating object is obtained from the global perspective information server and the sensor agent transmits the event line to the end recipient device.

As described in Claim 1 above, *Morris* discloses that its' system includes base computer 3 connected to database 7, which together facilitate the comparison and classification of event data. *Morris*, [0014]-[0017], [0020], [0078]. A PHOSITA would have understood base computer 3 in conjunction with database 7 constitutes the *global perspective information server* and base computer 3 constitutes the *end recipient device*. *Decl.*, ¶¶ 120-123. These components are depicted below in annotated Figure 1:



Morris, Fig. 1 (annotated).

Morris's global perspective information server is consistent with the disclosures of the '224 Patent. Particularly, the '224 Patent explains “[t]he 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.” ’224 Patent, 14:45-49. In *Morris*, base computer 3 and database 7 are a federated group of devices capable of supporting communications over a communication network which interoperate with remote computer 2, to compare and classify event data. *Decl.*, ¶¶ 120-123.

Shown above, “base computer 3 holds a database 7 with which the remote computers 2 can interact when the remote computers 2 run an object 4 to determine whether the object 4 is safe or unsafe.” *Morris*, [0078]. This “database 7 is populated, over time, with information relating to each object run on all of the connected remote computers 2.” *Id.* Base computer 3 compares “the data about the computer object received from the plural computers” and “classif[ies] the computer object as malware on the basis of said comparison.” *Id.*, [0016], [0017], [0081]-[0084] (describing process for determining object is “bad or unsafe”). Thus, *Morris* discloses a malware determination (i.e., *information associated with the one or more of the first object and the originating object*) is obtained by base computer 3 performing an analysis on the data stored in database 7. *Decl.*, ¶¶ 120-123. Thus, the

malware determination is obtained from base computer 3 and database 7 (i.e., *global perspective information server*). *Id.*; *Morris*, [0100] (“The centralisation of the community data in the community database 7 provides the ability to rapidly assimilate object behaviours, allowing for the rapid identification and determination of malware”).

Moreover, *Morris* discloses its “agent software” running on remote computer 2 (i.e., *sensor agent*) transmits the key comprising the event and contextual data (i.e., *event line*) to base computer 3 (i.e., *end recipient device*) to perform the above-described malware analysis. *Supra*, Claim [1(e)] ((further noting this key can be copied back to a local computer, another *end recipient*)).

8. Claim 13

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

Supra, Claim 4.

9. Claim 17

17[P]-[17(e)(iii)] A system for providing forensic visibility into a system, comprising: a first device comprising: a communication interface; a processor; data storage; and a sensor agent stored on the data storage that is executable by the processor, wherein the sensor agent is operable to: gather an event defining an action of a first object acting on a target; determine a global perspective for the event based on contextual state information for the event, wherein the global perspective relates to one or more other events related to the event across a network, and

Supra, Claim 10[P]-[10(e)(iv)].

[17(e)(iv)] wherein the contextual state comprises an indication of an originating object of the first object and an indication of at least one of 8 a second device on which the first object is executed and a user associated with the first object;

Morris discloses the contextual data includes the “Genesisactor” as an indication of an originating object of the first object. *Supra*, Claim [10(e)(ii)]. *Morris* further discloses that multiple remote computers run an object and send this data to the base computer 3/database 7 to determine whether that object is malware. *Supra*, Claim [1(c)(ii)]. Thus, *Morris* discloses obtaining contextual data concerning a second device on which the first object is executed.

Morris also discloses the contextual data can include “Identities” which “define the attributes of an object,” including “its logical location on the disk within the file system (its path)[.]” *Morris*, [0106]. A PHOSITA would have understood the files “path” would include user information associated with that file (i.e., *user associated with the first object*). *Decl.*, ¶¶ 126-129 (noting a complete file “path” identifies a user).

[17(e)(v)]-[17(e)(v)(ii)] generate an event line comprising information relating to the event, wherein the information relates to at least one of the first object, the action of the first object, the target, and the originating object; and transmit the generated event line utilizing the communication interface.

Supra, Claim [10(e)(vi)]- [10(e)(viii)].

⁸ This limitation recites a Markush group. *Supra*, Fn. 4.

B. Ground 2: Morris in view of Van Oorschot renders Claims 3 and 17 Obvious

Overview of Van Oorschot

Van Oorschot was filed on June 6, 2003 and issued on December 27, 2011 and therefore qualifies as prior art to the '224 Patent under 35 U.S.C. §§ 102(a)(1) and 102(a)(2). *Van Oorschot* (Ex. 1006). *Van Oorschot* was not cited or considered during prosecution of the '224 Patent.

Van Oorschot discloses an event management system which “record[s] a variety of system events initiated by a user.” *Van Oorschot*, 1:11-16. This event management system provides a “comprehensive security overview of activity within a given computer system” allowing a “forensic statement of the activity” to be generated. *Id.*, 3:65-66; *see also id.*, 1:37-43. To analyze event data, system events are logged in an “event log” and an event management tool normalizes this event data such that it can be interpreted and readily managed. *Id.*, 3:28-56. This event data can include several attributes, namely:

“‘who’ (the client initiating the event); ‘what’ (the type of event that was initiated); ‘when’ (the time at which the event occurred); ‘where’ (the system or device on which the event occurred); and ‘on what’ (the file, device, or setting that was accessed by the event)...[and] ‘where from’ (the identity of the client initiating the event) and ‘where to’ (the identity of the client acted upon by the event)”

Id., 3:57-4:17, Figs. 5A-5B.

Because *Van Oorschot*, like the '224 Patent, discloses methods for providing computer security by analyzing event data from potential threat events, *Van Oorschot* is in the same field of endeavor as the '224 Patent. *Compare Van Oorschot*, 1:37-43, 3:63-4:3 *with* '224 Patent, 1:17-20, 1:24-35; *Decl.*, ¶¶ 63-67. *Van Oorschot* is also directed at solving similar problems faced by the inventors of the '224 Patent, such as providing rules for handling security events. *Compare Van Oorschot*, 7:34-57, 9:4-17 *with* '224 Patent, 9:35-56, 13:39-51; *Decl.*, ¶¶ 63-67.

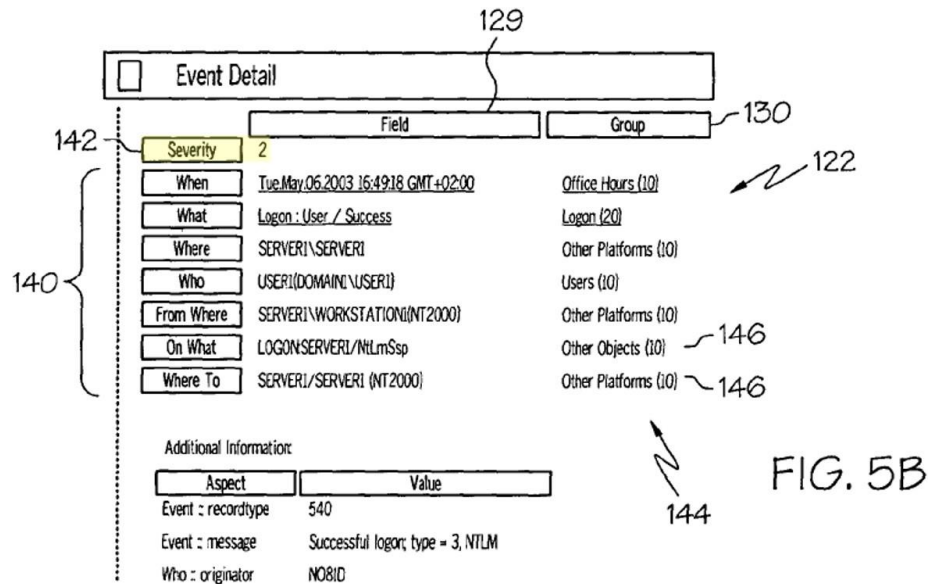
1. Claim 3

3. The method of claim 1, further comprising: obtaining an event priority based on one or more of the generated contextual state information and the global perspective, wherein the event line further includes the event priority.

While *Morris*'s methods include generating contextual information and a global perspective for an event and generating a key (i.e., *event line*), *see id.*, *Morris* does not expressly discuss obtaining an event priority based on one of these information types. *Van Oorschot* does.

Like the '224 Patent, *Van Oorschot* discloses “**assign[ing] a severity level**” to “system events” to determine an event priority. *Compare Van Oorschot*, 5:39-49, 7:34-57 (describing “policy rules” which can identify an event as a threat and assign a “severity level” for the threat), 9:4-17, 9:66-10:1 (noting a “severity level can be used as a sorting parameter”), Fig. 11 *with* '224 Patent, 9:35-56 (describing “rule set” which “may determine that an event meeting certain conditions be **assigned a**

priority according to a scale of severity”), 13:39-51, 22:31-56, Fig. 11. Van Oorschot’s “severity level” for an event is depicted below in Figure 5B:



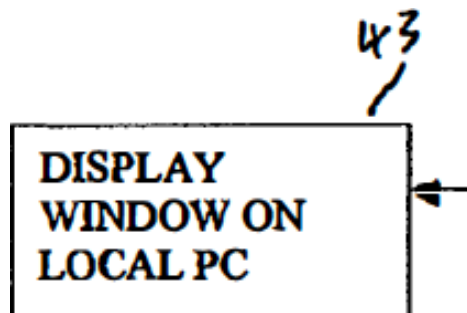
Van Oorschot, Fig. 5B (annotated).

This severity level is assigned *based on the generated contextual state information* related to the event. Van Oorschot discloses the event data and contextual data associated with an event is divided into groups; these groups are assigned a “significance factor;” and this factor “is used as a weighting...in later assigning of a severity level to an event[.]” *Id.*, 7:7-32. Policy or special attention rules are generated based on these groups, which define permitted and unpermitted actions within the security system. *Id.*, 7:33-36. These rules focus on permitted (or abnormal) activity related to certain attributes, such as “who” (e.g., “only ‘system administrators’ are permitted to modify files”) or “where” (e.g., “types of clients at

which the event can occur”)—i.e., the *generated contextual state* discussed above in claim 1. *Id.*, 7:21-57. These significance factors and rules are then analyzed when assigning the severity level for an event. *See generally, id.*, 8:12-10:1; *Decl.*, ¶¶ 131-136.

A PHOSITA would have been motivated to incorporate *Van Oorschot’s* assignment of event severity levels into *Morris’s* methods according to well-known benefits for prioritizing events—namely, focusing threat analysis on the most troublesome threats to conserve limited resources. *Decl.*, ¶¶ 131-146. And a PHOSITA would have appreciated a reasonable expectation of success making this modification. *Id.*, ¶ 138.

After this severity level is assigned to an event, a PHOSITA would have found it obvious to include this severity level in *Morris’s* key (i.e., *event line*) transmitted back to the local computer for display on a user’s display. *Id.*, ¶ 139 (further noting reasonable expectation of success making this simple modification). *Morris’s* local computers already comprise a “display window” for presenting information to a user. *Morris*, [0126]. This display is shown in the excerpt from Figure 4 below:



Id., Fig. 4 (excerpt). Including this severity level in the key (*event line*) transmitted back to the local computers for subsequent display would, as disclosed by Van Oorschot, “provide[] an additional gauge by which a decision can be made as to the manner in which an event is to be processed or as to the relative importance of the event.” Van Oorschot, 8:4-11; *Decl.*, 131-146. Indeed, Van Oorschot expressly contemplates displaying these event severity levels to a user to inform threat remediation tactics. See, e.g., Van Oorschot, Figs. 7-10; *Decl.*, 131-146. Morris in view of Van Oorschot therefore discloses *obtaining an event priority based on...the generated context...wherein the event line further includes the event priority.*

2. Claim 17

17[P]-[17(e)(iii)] A system for providing forensic visibility into a system, comprising: a first device comprising: a communication interface; a processor; data storage; and a sensor agent stored on the data storage that is executable by the processor, wherein the sensor agent is operable to: gather an event defining an action of a first object acting on a target; determine a global perspective for the event based on contextual state information for the event, wherein the global perspective relates to one or more other events related to the event across a network, and

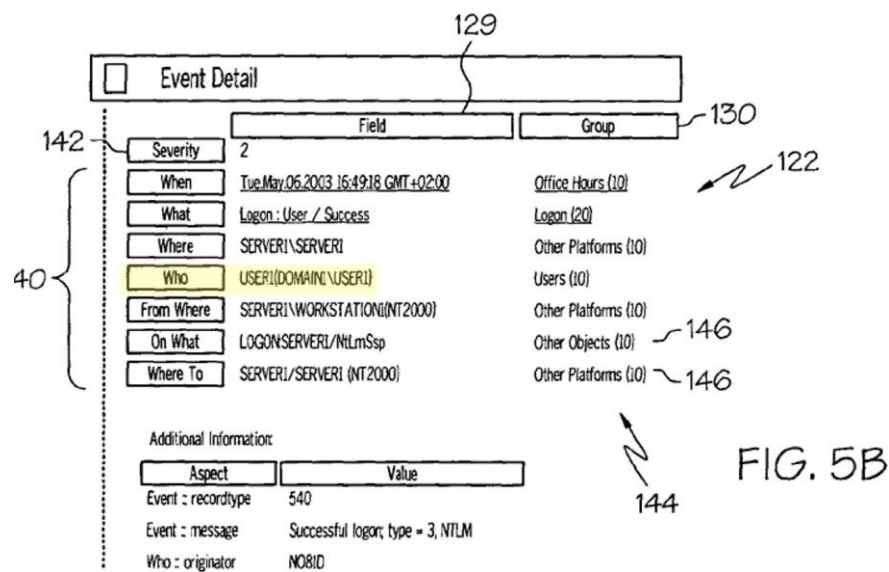
Supra, Claim 10[P]- [10(e)(iv)].

[17(e)(iv)] wherein the contextual state comprises an indication of an originating object of the first object and an indication of at least one of 9 a second device on which the first object is executed and a user associated with the first object;

To the extent Patent Owner argues Morris does not disclose an indication of

⁹ This limitation recites a Markush group. *Supra*, Fn. 4.

a user associated with the first object, Van Oorschot discloses a similar computer security system that captures event data comprising “seven attributes[,]” including “‘who’ (the user initiating the event)[.]” Van Oorschot, 6:14-23. A PHOSITA would have understood this discloses the claimed user associated with the first object. Decl., ¶¶ 148-154. This additional event data is highlighted below:



Van Oorschot., 5B (annotated); see also *id.* at Fig. 5A (depicting event data captured prior to normalization).

It would have been obvious to a PHOSITA to modify *Morris's* system to capture additional types of event data, such as “the user initiating the event” as disclosed by Van Oorschot. Decl., ¶¶ 148-154. It was a common principle in the art of computer security systems that gathering more detailed information from threats results in improved threat analysis and detection. *Id.* Indeed, “keeping additional

information about threats than what was previously available” provides “a more complete threat model[.]” *Id.* “To improve the quality and success ratio of back-end threat analysis,” malware analysis systems need to “collect[] more meta-data from the infected computer.” *Id.* Consistent with this reasoning, a PHOSITA would have been motivated to collect user information associated with an event to predictably improve the quality and success of *Morris’s* back-end threat identification and analysis. *Id.* Indeed, *Morris* teaches deriving additional metadata “not specifically mentioned” in its disclosure, including any combination of disclosed metadata elements and additional elements such that a PHOSITA would be further motivated by this express disclosure to derive additional metadata for subsequent analysis. *Id.*; *Morris*, [0110].

A PHOSITA would have understood that this combination of prior art elements would have been accomplished using known methods and with no change to their respective functions. *Decl.*, ¶¶ 148-154. For example, *Morris’s* system would derive the disclosed metadata associated with a threat event, such as the actor, event type, victim, Genesisactor, and would additionally derive user metadata associated with this event, as disclosed by *Van Oorschot*. *Id.* Because generating additional information about threats was a common way to provide more complete threat models for back-end analysis, there would have been a reasonable expectation of success configuring *Morris’s* system to collect user information along with the other

types of metadata from a threat event for later analysis. *Id.*

[17(e)(v)]-17(e)(vii) generate an event line comprising information relating to the event, wherein the information relates to at least one of the first object, the action of the first object, the target, and the originating object; and transmit the generated event line utilizing the communication interface.

Supra, Claim [10(e)(vi)]- [10(e)(viii)].

C. Ground 3: Capalik renders Claims 1-2, 4, 7-8, 10-13, and 16-19 Obvious

Overview of Capalik

Capalik was filed on June 17, 2011 and published on December 29, 2011 and therefore qualifies as prior art to the '224 Patent under 35 U.S.C. §§ 102(a)(1) and 102(a)(2). *Capalik* (Ex. 1008).

Capalik discloses “methods for analyzing malicious activities on a computer system[.]” *Capalik*, [0004]. An exemplary distributed computer system embodying these methods is depicted below in Figure 1:

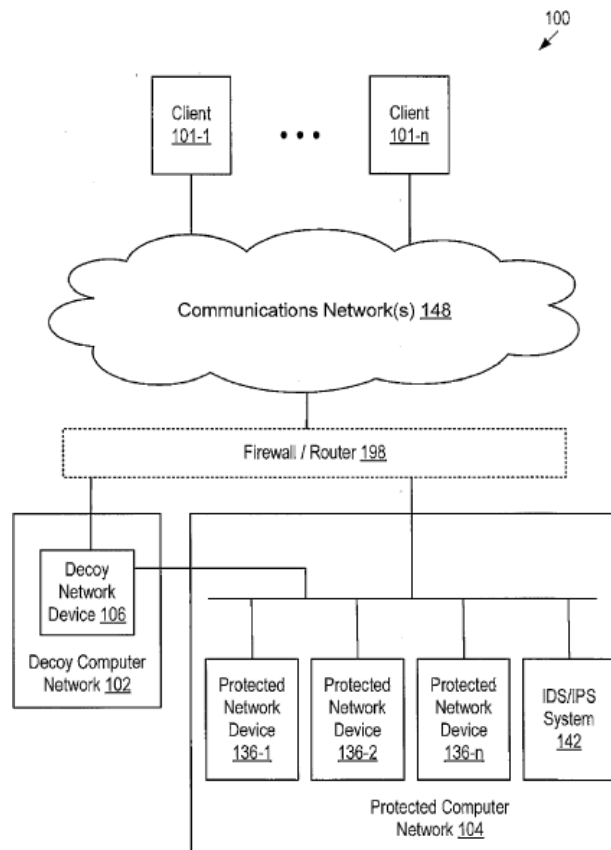


Figure 1

Id., Fig. 1. *Capalik's* computer system includes a “decoy computer network 102” comprising a “decoy network device 106” used “to collect fingerprint data of unauthorized activities.” *Id.*, [0030]; *see also id.*, Fig. 2 (depicting components of decoy network device). This decoy network device is “intentionally kept vulnerable to unauthorized or malicious activities” to “allow attackers to attack the decoy network device 106, so that the pattern of the attack can be monitored and analyzed to generate a fingerprint” *Id.*

This device captures “raw attack information” and communicates this information for storage into a database server “as forensic data [] for later analysis.”

Id., [0063]. This forensic attack data includes, for example, “an activity source,” “activity target,” “an action,” and an “association” such as “malignant, which represents that the activity source [] has modified the activity target [] to perform unauthorized activities[.]” *Id.*, [0080]-[0086]; *see also id.*, Fig. 5A (depicting block diagram illustrating exemplary data structures of unauthorized activity data). While *Capalik* discloses methods for monitoring activities on a decoy network, *Capalik* explains its methods “may be used for monitoring one or more non-decoy systems, such as the protected network device 136” depicted in Figure 1 above. *Id.*, [0032], [0067].

Because *Capalik*, like the ’224 Patent, discloses methods for providing computer security by analyzing event data from potential threat events, *Capalik* is in the same field of endeavor as the ’224 Patent. *Compare Capalik*, [0004], [0030], [0048] with ’224 Patent, 1:17-20, 1:24-26, 1:65-2:21; *Decl.*, ¶¶ 68-75. *Capalik* is also directed at solving similar problems faced by the inventors of the ’224 Patent, such as providing a forensic analysis of the impact of an attack on a target device. *Compare Capalik*, [0063] with ’224 Patent, 2:14-21, 2:25-29; *Decl.*, ¶¶ 68-75.

1. Claim 1

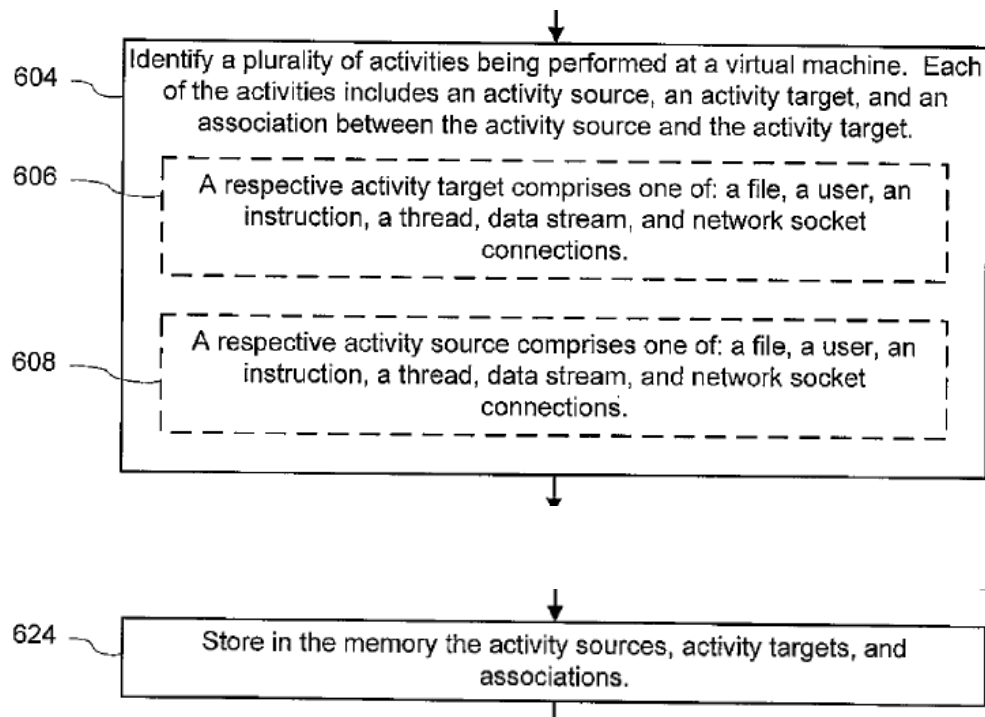
1[P]. A method comprising:

Capalik discloses “**methods** for protecting computer networks” including “**methods** for analyzing malicious activities on a computer system in order to better

protect the computer system from future malicious activity.” *Capalik*, [0004], Abstract; *see also id.*, Figs. 6A-6C (depicting flowcharts representing a method of identifying unauthorized activities on a computer system).

[1(a)] gathering an event defining an action of a first object acting on a target,

Capalik discloses methods for analyzing malicious activities on a computer system involving “monitoring activity on [a] virtual machine” such that a “**plurality of activities** performed at a virtual machine is identified[,]” including “an **activity source, activity target**, and an association between the activity source and the activity target.” *Capalik*, [0010]. The “activity sources, activity targets, and associations are stored in [] memory.” *Id.*; *see also id.*, [0063] (disclosing capturing “raw attack information” and storing in “database server 128 as forensic data 236 for later analysis”). This process for gathering an activity (i.e., *event*) including a source (i.e., *first object*) and an activity target (i.e., *target*) is depicted below:



Id., Figs. 6A and 6B (excerpts).

For example, *Capalik* discloses gathering the following event data:

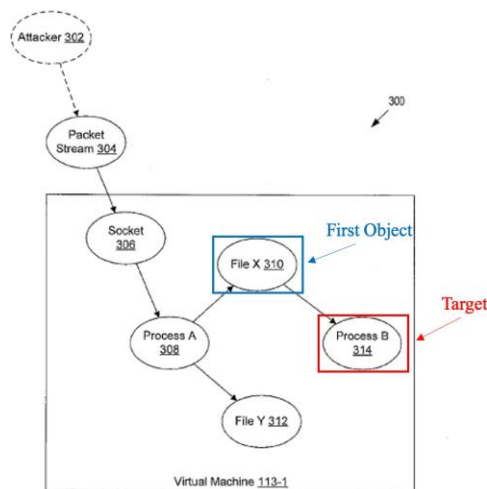


Figure 3D

Id., Fig. 3D (annotated); *see also id.*, Figs. 4A-4D (depicting similar unauthorized activity on files in a computer system), Fig. 4E (depicting unauthorized activity from multiple data streams). Figure 3D above illustrates an “exemplary network diagram[] representing unauthorized activity on a computer system (e.g., the virtual machine 113-1)[.]” *Id.*, [0067]. Here, a data Packet Stream 304 at a Socket 306 is monitored by the virtual machine. *Id.*, [0068]. Packet Stream 304 is directed to a Process A 308, which accesses File X 310, and File X 310 then initiates a Process B. *Id.*, [0069]. This diagram represents several related “activities” or “events”: (1) sending Packet Stream 304 into the computer system through Socket 306; (2) directing Packet Stream 304 to Process A; (3) Process A accessing Files X and Y; (4) File X initiating a Process B. *Decl.*, ¶¶ 157-161. For simplicity, only the final activity is annotated above, where File X boxed in blue (i.e., *first object*) performs an action of initiating a Process B boxed in red (i.e., *target*). *Id.* However, each of the four activities above comprises its own *first object* and *target*. *Id.*; *Capalik*, [0115] (explaining that Process A can be the activity target of one activity and the activity source of another activity).

This unauthorized activity data, including the sources, targets, and actions performed is stored in data structures, such as the one depicted below:

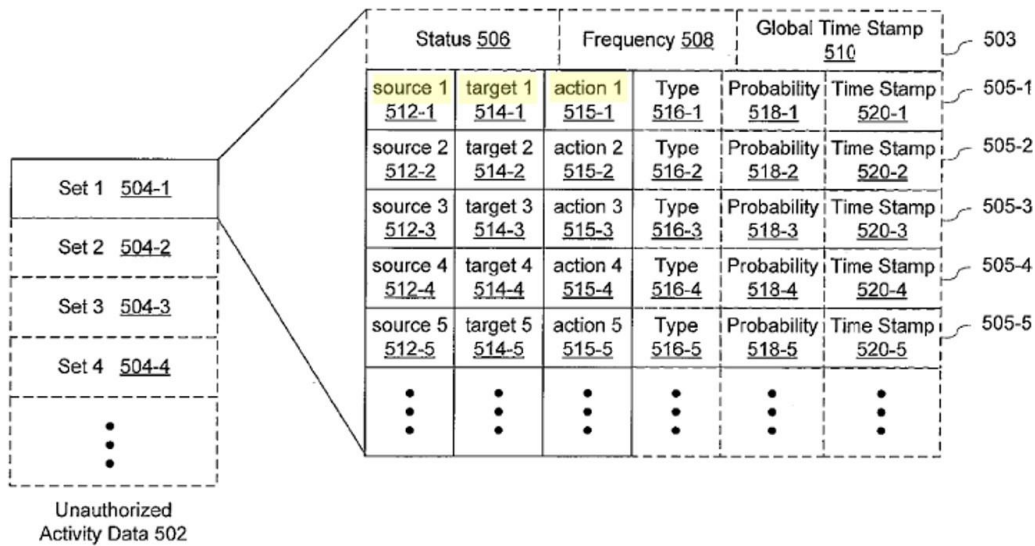


Figure 5A

Capalik, [0070, [0075], Fig. 5A (annotated). “Unauthorized activity data 502 includes unauthorized activity entries 505[,]” comprising: “**an activity source 512**, which calls, accesses, or executes the activity target 514;” “**an activity target 514**, which is called, accessed, or executed by the activity source 512[;]” and “**an action 515**,” which represents an “operation occurring between the activity source 512 and the activity target 514[,]” each highlighted above. *Id.*, [0075], [0081]-[0083]. Each entry can include “one or more” of a source, target, action, etc. *Id.*, [0080]. Thus, *Capalik* discloses gathering an event defining an action of a first object acting on a target.

[1(a)(i)] wherein the first object is executed on a device;

Capalik discloses the first object (e.g., File X 310) is executed on a virtual

machine. *Supra*, [1(a)] (depicted in Figure 3D). This virtual machine is stored on a “decoy network **device** 106,” depicted below:

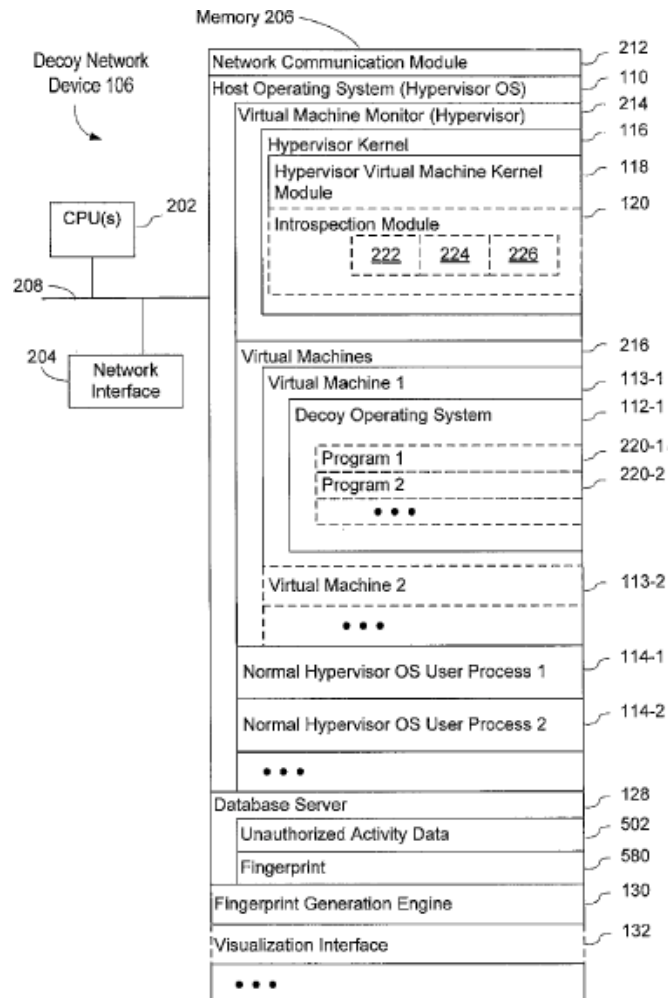


Figure 2

Capalik, Fig. 2.

[1(b)] generating contextual state information for the event by correlating the event to an originating object of the first object;

Capalik discloses gathering event data, including a first object acting on a target, such as the objects and targets identified in Figure 3D above. *Supra*, [1(a)].

Capalik discloses that once unauthorized activities are detected, “**related unauthorized activities are identified.**” *Capalik*, [0069]. For example, in Figure 3D, if “packet stream 304 and the socket 306 are identified as affected by unauthorized activities,” the chain of related events is identified. *Id.*, [0069]; *see also id.*, [0130] (describing *Capalik*’s methods generally providing the ability “to follow a chain of unauthorized activity”). In particular, as part of the chain of related events, *Capalik* discloses correlating an event to an originating object. *Decl.*, ¶¶ 163-166.

An originating object for the event in Figure 3D is depicted below, boxed in orange:

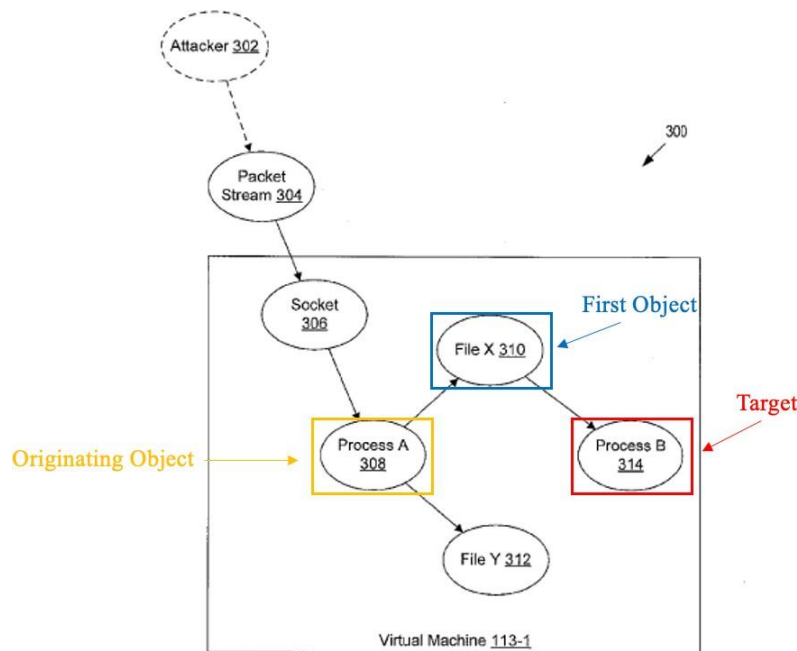


Figure 3D

Capalik, Figs. 3D (annotated); *Decl.*, ¶ 164. In this event, File X 310 initiates Process

B 314, and Process A 308 serves as the originating object—the process which accesses file X 310 in the related activity chain. *Id.* The overall activity chain runs as follows: “[T]he unauthorized activities send the packet stream 304 into the computer system [] through the socket 306; the packet stream 304 is directed to the process A 308[.]” *Capalik*, [0070]. Process A “is treated as affected by unauthorized activities...[and then] process A 308 accesses a file X 310 and a file Y 312, and both the file X 310 and the file Y 312 are treated as affected by unauthorized activities.” *Id.*, [0069]. “Thereafter, the file X 310 initiates a process B 314, and the process B is treated as affected by unauthorized activities.” *Id.* Based on this disclosure, a PHOSITA would have understood that *Capalik* correlates an event to its originating object by tracking the related chain of unauthorized activities. *Decl.*, ¶¶ 163-166.

In view of the foregoing, *Capalik* discloses *generating contextual state information for the event by correlating the event to an originating object of the first object.*

[1(c)] obtaining a global perspective for the event based on the contextual state information,

The '224 Patent explains that “obtaining a global perspective for the at least one event” based on the contextual state information includes “obtaining information associated with one or more of the first object and the originating object” such as “a determination as to whether the first object is malware” and “a determination as to

whether the originating object is malware.” ’224 Patent, 4:45-59, 5:11-16, 9:26-28, 17:56-66; *see also id.*, claim 8 (claiming global perspective comprising a malware determination for the first and/or originating objects).

Capalik discloses determining whether the first and/or originating objects are malware. Specifically, *Capalik* discloses determining “association types” between sources and targets, such types including “**malicious associations** v. benign associations[.]” *Capalik*, [0075]. Unauthorized activity data can be grouped in the following data structure:

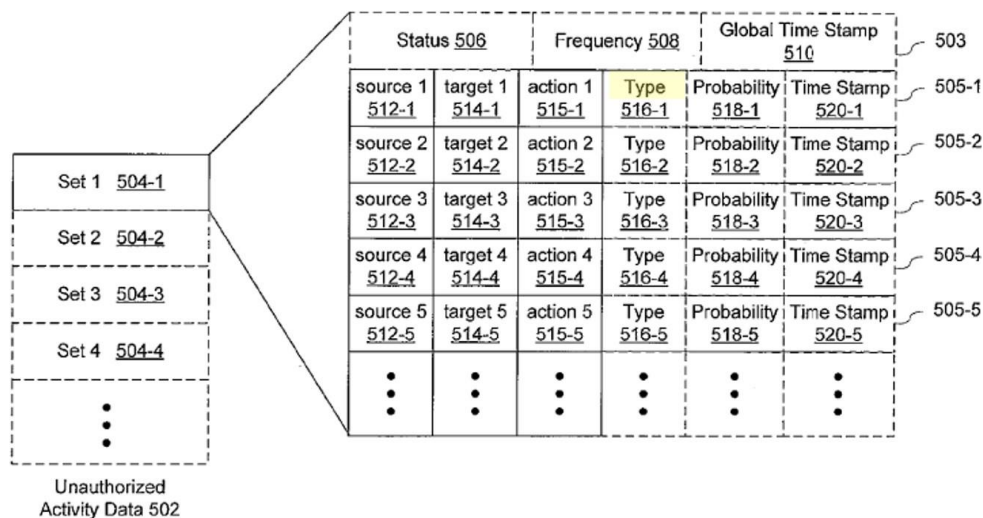


Figure 5A

Id., Fig. 5A (annotated). “Each set 504 in the unauthorized activity data 502 in Fig. 5A [] includes one or more unauthorized activity entries” which comprises, in relevant part, “an activity source 512[;]” “an activity target 514[;]” “an action, 515, which represents an...operation occurring between the activity source 512 and the

activity target[;]” and optionally an “**association, type 516**, which when identified, represents the type of association between the activity source 512 and the activity target 514[.]” *Id.*, [0080]-[0084]. This “type” (highlighted above) may be identified as “**malignant**, which represents that the activity source 512 has modified the activity target 514 to perform unauthorized activities[.]” *Id.*, [0084]-[0085].

Capalik discloses determining malicious or malignant associations between sources and targets in the events occurring on virtual machine 113-1, as follows:

“as shown in FIG. 3C, the process A 308 modifies the file X 310, performing unauthorized activities (e.g., **corrupting data or writing a malicious code**). **The process A 308, as an activity source to the file X 310, causes unauthorized activities on the file X 310.** By identifying that the process A 308 performed unauthorized activities, **the process A 308 is determined to be affected by the unauthorized activities, and the association between the socket 306 and the process A 308 is determined to be malicious** (i.e., unauthorized).”

Id., [0106]. A PHOSITA would have understood determining Process A to be “malicious” by, for example, writing “**malicious code**,” includes determining Process A (i.e., *originating object*) to be malware. *Decl.*, ¶¶ 167-172. And once Process A is determined to contain malicious code, as Process A accesses File X (i.e., *first object*), File X is determined to be malware. *Id.* This is consistent with the ’224 Patent’s definition for “malware,” which “refer[s] generally to any executable computer file or, more generally ‘object’, that is or contains **malicious code**...” ’224

Patent, 2:3-7. Thus, *Capalik* discloses obtaining a global perspective for the event based on the contextual state information.

[1(c)(i)] wherein the global perspective comprises information associated with one or more of the first object and the originating object,

Capalik discloses the global perspective comprises information associated with one or more of the first object and the originating object—namely, a determination as to whether the first and/or originating objects are malware. *Supra*, [1(c)].

[1(c)(ii)] and wherein the global perspective relates to one or more other events related to the event across a network;

Capalik discloses obtaining a global perspective for an event, including malware determinations for a first and/or originating object. *Supra*, Claim [1(c)]. *Capalik* further discloses that “the methods described herein need not be restricted to analysis of a single virtualized operating system, but, rather, **are able to follow a chain of unauthorized activity across multiple virtualized operating systems.**” *Capalik*, [0130]. This enables “identifying and thwarting advanced threats that involve multiple attackers spread across multiple systems[.]” *Id.* A PHOSITA would have understood that in an attack across multiple virtualized operating systems, *Capalik’s* methods would follow the related chain of unauthorized activity across each operating system and would perform the methods identified above for obtaining a global perspective—namely, determining “association types” between sources and

targets, including “malicious associations.” *Decl.*, ¶¶ 175-177. In this way, *Capalik*’s disclosed methods include obtaining a global perspective for an event that relates to a related event across a network, including a malware determination for the first and/or originating objects. *Id.*

Additionally, *Capalik* discloses obtaining global perspective information in a scenario based on related events from multiple data streams across a network, shown in annotated Figure 4E below:

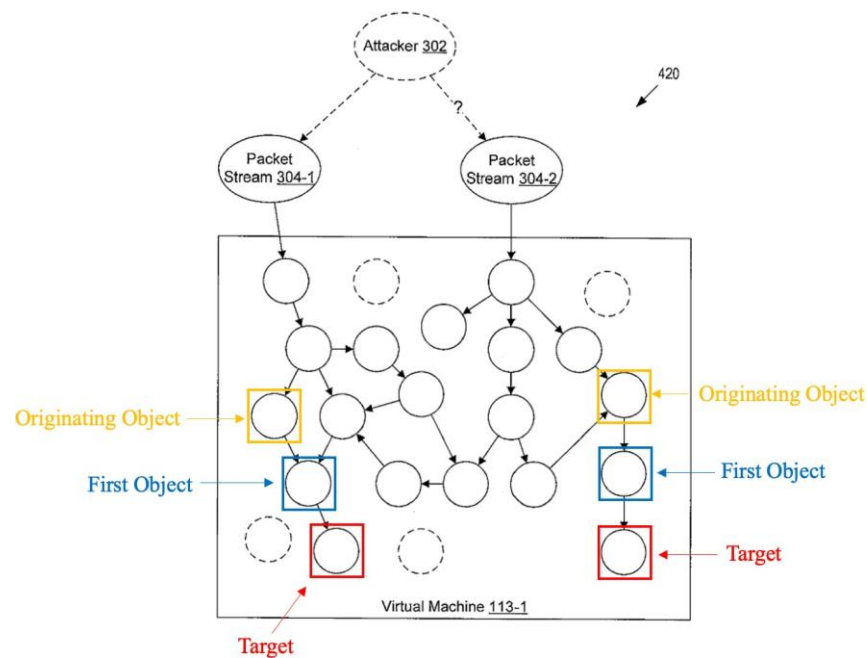
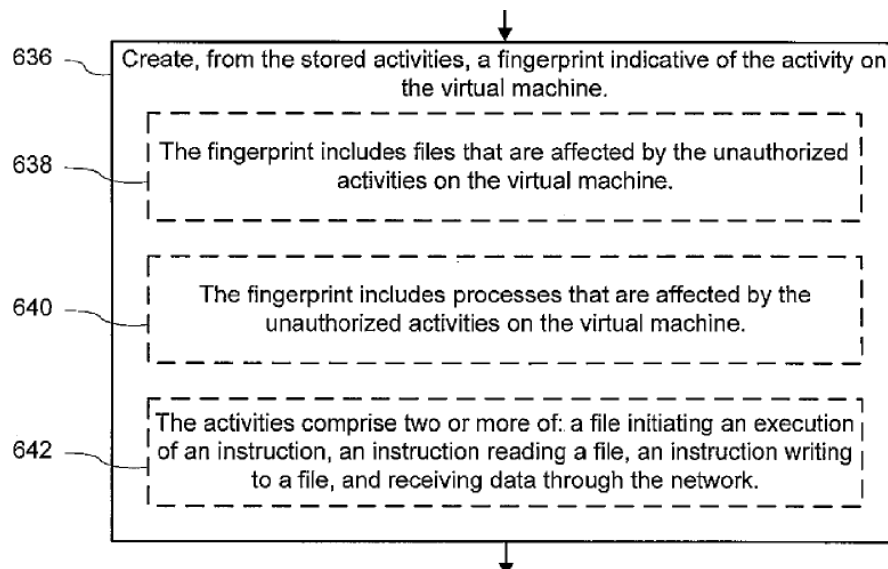


Figure 4E

Capalik, Fig. 4E (annotated). Here, *Capalik*’s methods include making a malware determination for the originating and/or first objects. *Supra*, [1(c)(i)-(ii)]; *Decl.*, ¶ 177.

[1(d)] generating an event line comprising information relating to the event,

Capalik discloses after obtaining the above activity information and associated data, “[a] **fingerprint indicative of the activity on the virtual machine is created from the stored activities.**” *Capalik*, [0010]. The “fingerprint is transmitted to one or more other computer systems on the network to prevent future attacks that comprise the same or similar activities as indicated by the fingerprint.” *Id.*; see also *id.*, [0063] (describing fingerprint generation engine 130 for generating signature of an attack). This fingerprint generation process is shown below in excerpted Fig. 6C:



Id., Fig. 6C (excerpt).

[1(d)(i)] wherein the information relates to at least one of the first object, the action of the first object, the target, and the originating object; and

Capalik discloses the fingerprint includes stored activity data, including the files and/or processes that were affected by unauthorized activities on the virtual machine. *Capalik*, [0121]-[0122]. Specifically, Figure 5B below “illustrates an exemplary data structure of fingerprint 580”:

580-1
↙

Status 506				
source 1 512-1	target 1 514-1	Type 516-1	Time Stamp 520-1	505-1
source 2 512-2	target 2 514-2	Type 516-2	Time Stamp 520-2	505-2
source 3 512-3	target 3 514-3	Type 516-3	Time Stamp 520-3	505-3
source 4 512-4	target 4 514-4	Type 516-4	Time Stamp 520-4	505-4
source 5 512-5	target 5 514-5	Type 516-5	Time Stamp 520-5	505-5
⋮	⋮	⋮	⋮	

Figure 5B

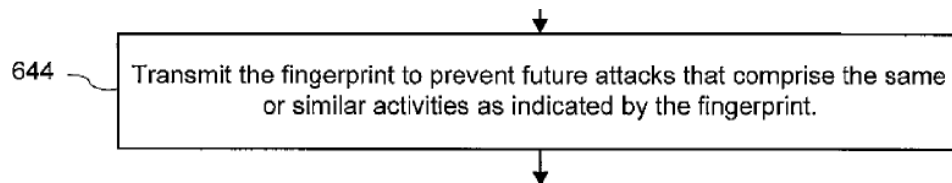
Id., Fig. 5B. Fingerprint 580 includes “an **activity source 512**, an **activity target 514**, an (optional) association type 516, and an (optional) time stamp 520” (i.e., *information uniquely identifying the first object and the target*). *Id.*, [0090]. *Capalik* also discloses the fingerprint can store “**branching information**” (see *Capalik*,

[0099]) along with “(one or more) activity sources 512,” including “respective pairs of activity sources...when the association type for a respective pair is malignant.” *Id.*, [0092]-[0094]. A PHOSITA would have understood this “branching information” and/or multiple activity sources and pairs of activity sources would include the *originating object* of the first object. *Decl.*, ¶¶ 180-184.

Capalik also discloses that “fingerprint 580 includes one or more of...raw network information collected from a respective virtual machine 113 or a respective decoy operating system 112[.]” *Id.*, [0099]. A PHOSITA would have understood this includes storing any of the raw attack information originally stored in memory, such as the attack information identified in Figure 5A. *Decl.*, ¶¶ 180-184; *Capalik* [0120] (further disclosing “collecting additional data associated with the activity sources 512”). This includes, for example, the “**action 515**” which represents an “operation occurring between the activity source 512 and the activity target 514.” *Supra*, [1(a)]. Thus, *Capalik* discloses *generating an event line comprising information relating to the event (fingerprint 580) including details associated with the at least one event, the details including information relating to at least one of the first object (activity source 512), the action of the first object (action 515), the target (target 514), and the originating object (branching information/multiple activity sources).*

[1(e)] transmitting the generated event line.

Supra, [1(d)] (describing transmitting fingerprint). This process is shown below in excerpted Figure 6C:



Id., Fig. 6C (excerpt); *see also id.*, [0126] (describing transmitting fingerprint to “protected network devices 136” or to “the IDS/IPS system 142”).

2. Claim 2

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.

Capalik discloses obtaining information associated with the first and/or originating object, such as a malware determination for the first/originating object. *Supra*, Claim [1(c)].

Capalik further discloses the activity data above is stored in a “**database server 128** as forensic data 236 for later analysis.” *Supra*, Claim [1(a)] (discussing *Capalik*, [0063]). The decoy network device stores “the activity sources, activity targets, and associations in...database server 128[.]” *Id.*, [0112]. This database server 128 can be stored on decoy network device 106, or “located outside the decoy network device 106.” *Capalik*, [0055]. A PHOSITA would have understood

database server 128 is a *community database* because it stores “chain[s] of unauthorized activity across **multiple** virtualized operating systems” or data from “multiple packets of data streams[,]” which includes unauthorized activity from multiple attackers, multiple devices, or multiple data streams. *Decl.*, ¶¶ 186-188; *Capalik*, [0074], [0130].

Capalik additionally discloses transmitting its fingerprint 580 “to one or more other computer systems on the network[,]” to protected network devices 136, or the IDS/IPS system 142 (i.e., each representing an *end recipient*). *Id.*, [0011]; *supra*, Claim [1(e)].

3. Claim 4

4. The method of claim 1, wherein the event includes information identifying the first object performing the action, information identifying the action being performed, and information identifying the target upon which the act is being performed.

Capalik discloses gathering event information, including the activity data depicted below:

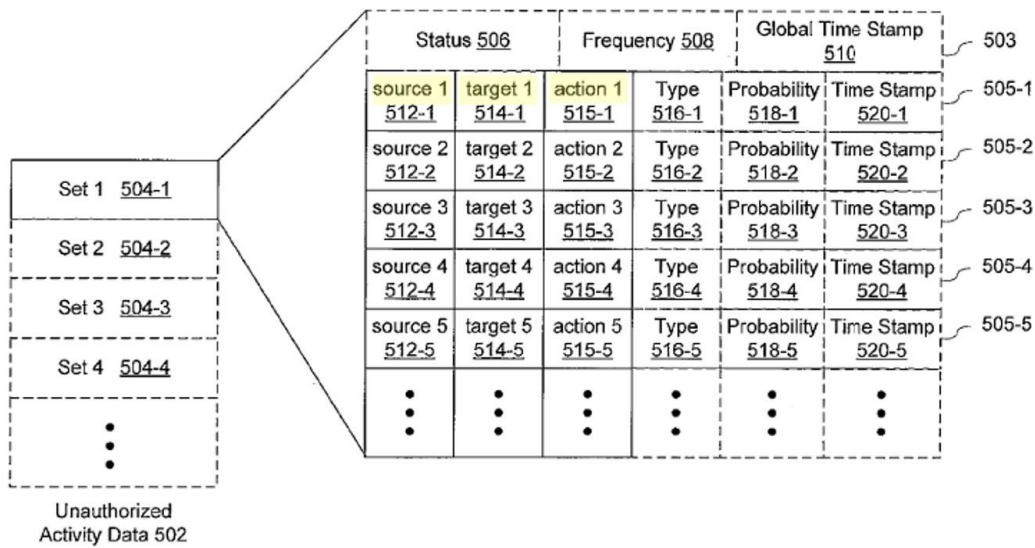


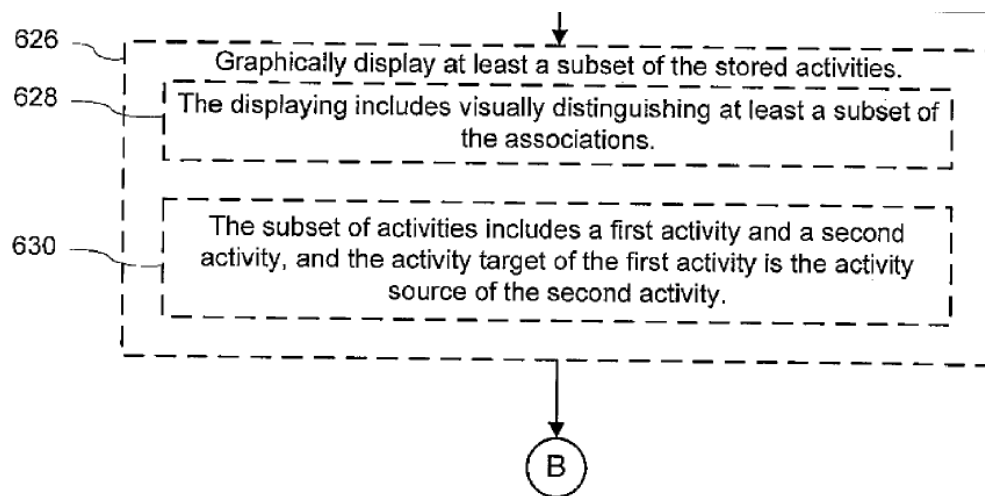
Figure 5A

Capalik, Fig. 5A (annotated); *Supra*, Claim [1(a)]. This includes “unauthorized activity entries 505,” comprising: “**an activity source 512**, which calls, accesses, or executes the activity target 514;” “**an activity target 514**, which is called, accessed, or executed by the activity source 512[;]” and “**an action 515**,” which represents an “operation occurring between the activity source 512 and the activity target 514[;]” each highlighted above. *Id.*

4. Claim 7

7. *The method of claim 4, further comprising: heuristically displaying the information identifying the first object performing the action, the information identifying the action being performed, the information identifying the target upon which the act is being performed, and information associated with the global perspective according to one or more of: a location associated with the first object...*

Capalik discloses its methods further include “**displaying** at least a subset of the activities (e.g., **action sources**, **action targets**, and **actions**).” *Capalik*, [0011]. The process for graphically displaying activity data is shown in excerpted Figure 6B below:



Id., Fig. 6B (excerpt). *Capalik* discloses this graphical representation can be “an activity diagram as shown in FIGS. 3A-3D and 4A-4E[,]” examples of which are provided above. *Id.*, [0113].

For example, with respect to Figure 4E, *Capalik* discloses “[w]hen the type of

associations is identified (e.g., malignant, benign, etc., as described in more detail below with reference to a type 516 in FIG. 5A), at least a subset of **the associations can be visually distinguished** (e.g., **a respective bold arrow representing a malignant association...**” *Id.*, [0074]. A PHOSITA would have understood this includes displaying a *global perspective according to...a location associated with a first object. Decl.*, ¶¶ 190-194. Here, a source (i.e., *first object*) is determined to be malicious based on its location in a chain of unauthorized activity. *Id.* In annotated Figure 4E below, if the originating object (boxed in orange) is determined to perform unauthorized activities, then the bold arrow pointing to the first object (boxed in blue) visually identifies this “malignant association” such that the first object is similarly identified as performing unauthorized activities:

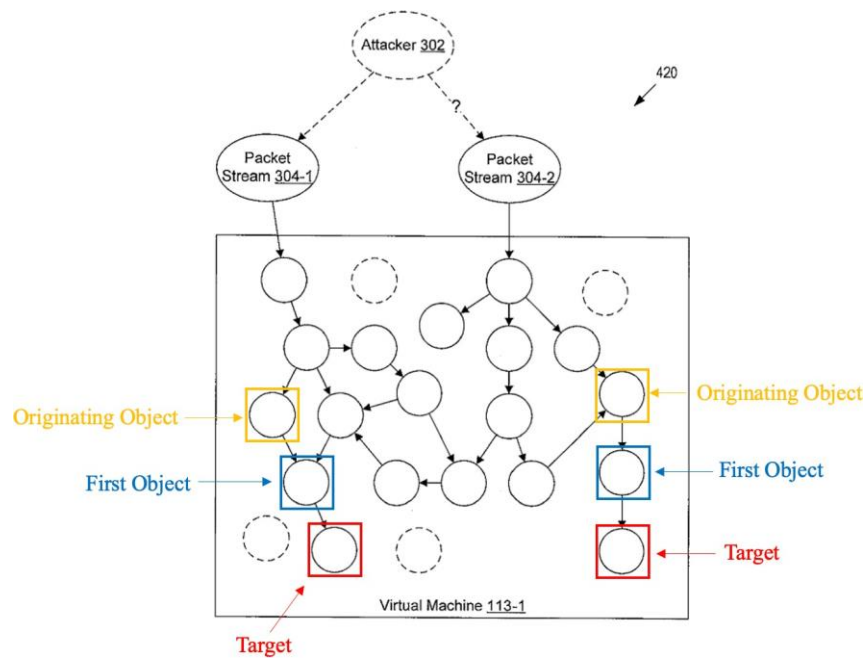


Figure 4E

Id., ¶ 193 *Capalik* thus discloses *heuristically displaying information identifying the first object performing the action, information identifying the action being performed, information identifying the target upon which the act is being performed, and the global perspective according to one or more of a location associated with the first object.*

5. Claim 8

8. The method of claim 1, wherein the global perspective comprises information comprises at least one of: an age; a popularity; a determination as to whether the first object is malware; a determination as to whether the originating object is malware; an Internet Protocol (IP) Address; and a Uniform Resource Locator (URL).

Supra, claim [1(c)] (describing determination that first and/or originating objects are malware).

6. Claim 10

10[P]. A system for providing forensic visibility into a system, comprising:

Capalik discloses “**systems** and methods for protecting computer networks” including “**systems** and methods for analyzing malicious activities on a computer system in order to better protect the computer system from future malicious activity.” *Capalik*, [0004], Abstract; *see also id.*, Fig. 1 (depicting distributed computer system). This system “generates and retrieves forensic data (or fingerprint)” relating to system events. *Id.*, [0048]; *see also id.*, [0063] (analyzing “raw forensic information” for a “forensic analysis”).

[10(a)] a device comprising:

Supra, Claim [1(a)(i)] (depicting **decoy network device 106**).

[10(b)] a communication interface;

Capalik discloses the decoy network device includes “one or more **network or other communications interfaces 204** [.]” *Capalik*, [0033], Fig. 2.

[10(c)] a processor;

Capalik discloses the decoy network device includes “one or more **processing units (CPUs)**[.]” *Capalik*, [0033], Fig. 2.

[10(d)] data storage; and

Capalik discloses the decoy network device includes “**memory 206**[.]” *Capalik*, [0033], Fig. 2; *see also id.*, [0034] (describing memory 206 as DRAM, SRAM, DDR RAM, non-volatile memory, etc.).

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

Capalik discloses “memory 206” stores a set of modules, including a network communications module 212, host operating system 110, database server 128, fingerprint generation engine 130, and visualization interface 132. *See generally Capalik*, [0034]-[0053]. These modules are collectively a *sensor agent* executable by CPU 202 operable to perform the claimed functions. *Decl.*, ¶ 202. A PHOSITA would have understood each module may collectively be implemented as a single software agent. *Id.*; *Capalik*, [0054] (disclosing the “modules...need not be implemented as separate software programs” such that they can be “combined or otherwise re-arranged”).

The remaining limitations of Claim 10 are substantively identical to method steps of Claim 1 and are rendered obvious for the same reasons detailed in Claim 1.

7. Claim 11

11. The system of claim 10, wherein the event is executed by the processor.

Capalik renders obvious the system of claim 10. *Supra*, Claim 10. A PHOSITA would have understood the decoy network device’s CPU would execute the events described above. *Decl.*, ¶ 204.

8. Claim 12

12. The system of claim 10, further comprising: a global perspective information server; and an end recipient device, wherein the information associated with the one or more of the first object and the originating object is obtained from the global perspective information server and the sensor agent transmits the event line to the end recipient device.

While *Capalik* generally discusses the functions of claim 10's system effectuated by the modules of the decoy network device 106, *Capalik* explains these functional elements can be “grouped or split among various components.” *Capalik*, [0055]. These functional elements are depicted below:

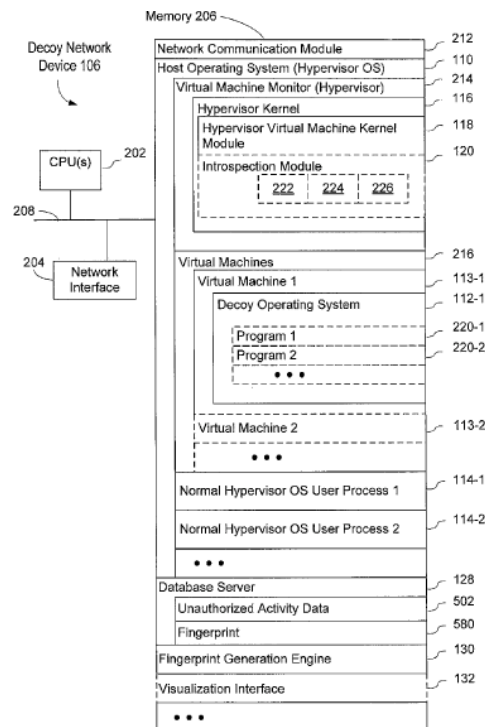


Figure 2

Id., Fig. 2.

Capalik contemplates splitting these modules into “distinct computing

devices” such that one or more blocks of Figure 2 can be “**implemented on one or more servers** designed to provide the described functionality.” *Id.*, [0056]. In such configurations, a PHOSITA would have understood the server would optionally include functions of the introspection module to determine associations between data components such that this server constitutes a *global perspective information server*—i.e., it generates information associated with a malware determination (type 516). *Decl.*, ¶¶ 205-206. Decoy network device 106 would then obtain this information from the server and include it in the fingerprint for transmission by the sensor agent to an end recipient device (e.g., protected device, IDS/IPS) as discussed above in claim 2. *Id.*

9. Claim 13

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

Supra, Claim 4.

10. Claim 16

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

Capalik discloses its decoy network device heuristically displays the above claimed information. *Supra*, Claim 7. While this claim recites “the end recipient device” heuristically displays this information, there is no “end recipient device” found in claims 10 or 13 from which this claim depends. To the extent this claim requires another device to heuristically display this information, as described above, *Capalik* discloses transmitting fingerprint 580 “to one or more other computer systems on the network[.]” *Supra*, [1(d)]. This includes a client computer system 101, depicted in Figure 1 below:

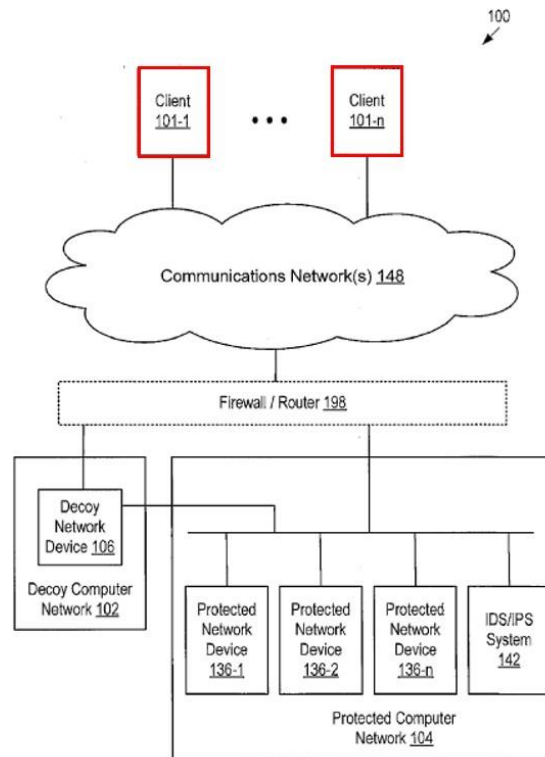


Figure 1

Id., Fig. 1 (annotated). *Capalik* discloses its decoy network device prepares the fingerprint event data “for display” such as “on a GUI of a client 101.” *Id.*, [0039].

11. Claim 17

17[P]-[17(e)(iii)] A system for providing forensic visibility into a system, comprising: a first device comprising: a communication interface; a processor; data storage; and a sensor agent stored on the data storage that is executable by the processor, wherein the sensor agent is operable to: gather an event defining an action of a first object acting on a target; determine a global perspective for the event based on contextual state information for the event, wherein the global perspective relates to one or more other events related to the event across a network, and

Supra, Claim 10[P]- [10(e)(iv)].

[17(e)(iv)] wherein the contextual state comprises an indication of an originating object of the first object and an indication of at least one of a second device on which the first object is executed and a user associated with the first object;

Supra, claim [1(b)] (describing generating a contextual state including an indication of the originating object of the first object, boxed above in Figure 3D in orange and blue, respectively). *Capalik* further discloses in embodiments, “a respective activity source” can be “a **user**” (i.e., *a user associated with the first object*). *Capalik*, [0104]; *see also id.*, [0105] (disclosing a target can similarly be “a user”). A PHOSITA would have understood *Capalik*’s methods include an indication of a user associated with the first object in embodiments where an activity source or activity target is a “user.” *Decl.*, ¶¶ 213-215.

[17(e)(v)]-17(e)(vii)] generate an event line comprising information relating to the event, wherein the information relates to at least one of the first object, the action of the first object, the target, and the originating object; and transmit the generated event line utilizing the communication interface.

Supra, Claim [10(e)(vi)]- [10(e)(viii)].

12. Claim 18

18. The system of claim 17, further comprising a global perspective information server comprising: a processor; a communication interface; data storage; and a global perspective module, wherein the global perspective module is operable to: receive the event line from the device; assemble a second event line including details associated with the event, wherein the second event line comprises information identifying the first object, information identifying the action of the first object, information identifying the target, and information identifying the originating object; and transmit the second event line utilizing the communication interface to an end recipient.

As discussed above, *Capalik* discloses implementations where the modules of

decoy network device 106 are split into multiple components, including a first component and a server (i.e., *global perspective information server*). *Supra*, claim 12. A PHOSITA would have understood the server would include its own *processor*, *communication interface*, and *data storage* to effectuate the receipt of unauthorized activity data and generation of a fingerprint. *Decl.*, ¶¶ 217-218. A PHOSITA would also have understood this server would include a *global perspective module* to receive the unauthorized activity data from the monitor device (i.e., *first event line*) and assemble a *second event line* to transmit over the network to an *end recipient*, such as a protected network device, an IDS/IPS, or a client 101. *Id.* This second event line would comprise the *information identifying the first object*, *information identifying the action of the first object*, *information identifying the target*, and *information identifying the originating object*. *Id.*; *supra*, claim [1(d)(i)].

13. Claim 19

19. The system of claim 18, wherein the end recipient heuristically displays the information identifying the first object, the information identifying the action of the first object, the information identifying the target, and information associated with the global perspective according to one or more of: a location associated with the first object...

Supra, claim 16.

D. Ground 4: Capalik in view of Van Oorschot renders Claims 3 and 17 Obvious

1. Claim 3

3. The method of claim 1, further comprising: obtaining an event priority based on one or more of the generated contextual state information and the global perspective, wherein the event line further includes the event priority.

Capalik discloses its decoy network device can “determine[] a probability of a respective association” which “represents [the] likelihood that the association is malignant (or benign)...” *Capalik*, [0118]; *see also id.*, [0088], Fig. 5A (depicting probability 518). This “probability” can be used to adjust a “monitoring priority.” *Id.*, [0119]. While *Capalik* discloses assigning a priority to adjust how events are monitored, *Van Oorschot* discloses “**assign[ing] a severity level**” to “system events” based on the generated context to inform the manner in which an event is to be processed. *Supra*, Ground 2, claim 3. A PHOSITA would have been motivated and would have appreciated a reasonable expectation of success modifying *Capalik*’s malware detection methods to incorporate *Van Oorschot*’s known event priority severity level assignment to appreciate the benefits outlined in Ground 2 above. *Supra*, Ground 2, Claim 3. In *Capalik*’s modified methods, after gathering event information, generating contextual information and obtaining a global perspective as described above, *supra*, claim 1, *Capalik*’s system would incorporate *Van Oorschot*’s assignment of severity levels to inform a recipient of the relevance of the event. *Decl.*, ¶¶ 220-225.

It would have been obvious to a PHOSITA to include the event priority in *Capalik's* fingerprint to identify the significance of an event because this would provide additional guidance when responding to events. *Decl.*, ¶¶ 220-225. There would have been a reasonable expectation of success modifying *Capalik's* signature to include well-known event priority information, as exemplified by *Van Oorschot*. *Id.*

2. Claim 17

17[P]-[17(e)(iii)] A system for providing forensic visibility into a system, comprising: a first device comprising: a communication interface; a processor; data storage; and a sensor agent stored on the data storage that is executable by the processor, wherein the sensor agent is operable to: gather an event defining an action of a first object acting on a target; determine a global perspective for the event based on contextual state information for the event, wherein the global perspective relates to one or more other events related to the event across a network, and

Supra, Claim 10[P]- [10(e)(iv)].

[17(e)(iv)] wherein the contextual state comprises an indication of an originating object of the first object and an indication of at least one of a second device on which the first object is executed and a user associated with the first object;

To the extent Patent Owner argues *Capalik* does not disclose *an indication of at least one of a device on which the first object is executed and a user associated with the first object*, *Van Oorschot* does for the reasons discussed in Ground 1 above. *Supra*, Ground 1, Claim 17(e)(iv) (describing *Van Oorschot's* similar computer security system which captures event data including “‘**who**’ (the user initiating the event)” and “‘**where**’ (the system or device on which the event occurred)”); see

also *Van Oorschot*, Figs. 5A-5B.

It would have been obvious to a PHOSITA to modify *Capalik's* system to capture additional event metadata, including “where” (i.e., the “device on which the event occurred”) and “who” (i.e., “the user initiating the event”) for the reasons outlined above in Ground 1. *Supra*, Ground 1, Claim 17(e)(iv). Namely, this combination adheres to recognized computer security principles—i.e., gathering more detailed threat information provides improved threat analysis and detection where limited data acquisition can hinder back-end performance and result in unperceived threats. *Decl.*, ¶¶ 227-231. A PHOSITA would have been motivated to collect device and user information associated with an event to predictably improve the quality and success of *Capalik's* back-end threat identification and analysis. *Id.* And like *Morris*, *Capalik* discloses that “additional...data structures not described above” related to activity data can be stored in memory for analysis. *Capalik*, [0054]; see also *id.*, [0120] (disclosing “collecting additional data associated with the activity sources” to create a fingerprint from this data). Based on this disclosure, a PHOSITA would have been expressly motivated to collect and store additional data, such as the device where the event occurred and the user initiating the event. *Decl.*, ¶¶ 227-231.

As above, a PHOSITA would have understood this combination of prior art elements would have been accomplished using known methods with no change to

their respective functions. *Id.* Capalik's system would simply derive additional activity data in addition to the disclosed data and a PHOSITA would have appreciated a reasonable expectation of success making this routine modification. *Id.*

[17(e)(v)]- 17(e)(vii)] generate an event line comprising information relating to the event, wherein the information relates to at least one of the first object, the action of the first object, the target, and the originating object; and transmit the generated event line utilizing the communication interface.

Supra, Claim [10(e)(vi)]- [10(e)(viii)].

V. DISCRETIONARY DENIAL IS NOT WARRANTED

A. The Advanced Bionics Framework Favors Institution Under § 325(d)

Under the *Advanced Bionics* framework applying the *Becton-Dickinson* factors, the Board first considers whether the same or substantially the same prior art or arguments were previously presented to the office. *Advanced Bionics, LLC v. MED-EL Elektromedizinische Geräte GmbH*, IPR2019-01469, Paper 6 at 8 (PTAB Feb. 13, 2020) (precedential) (“*Advanced Bionics*”). The first condition of the *Advanced Bionics* framework is not satisfied and discretionary denial under §325(d) is not appropriate.

Petitioner is merely seeking to join this petition with *CrowdStrike, Inc. v. Webroot Inc.*, Case No. IPR2023-00126 (“CrowdStrike IPR”), which was instituted May 5, 2023. The CrowdStrike IPR petition presents four new grounds of

unpatentability relying on three new prior art references: *Morris*¹⁰, *Capalik*, and *Van Oorschot*. While none of these references were cited or considered by the Examiner, a different *Capalik* publication (*Capalik* '570) was considered during prosecution. *Capalik* '570 was applied as a secondary reference by the Examiner in an initial rejection. The Examiner rejected then-pending claims 1-20 over *Kumar* in view of *Capalik* '570, and reliance on *Capalik* '570 was limited to assembling and transmitting the claimed *event line*. See '224 Patent File History, 102-103. As Applicant admitted during prosecution, *Capalik* '570 was not used as a primary, as Petitioner's relied-upon *Capalik* reference is here, to teach the majority of the claims. *Id.*, 293 ("the Office Action does not allege that *Capalik* teaches the above claim elements but rather cites *Capalik* with respect to other claim elements. *Capalik* relates to capturing unauthorized intrusions into a computer using a hypervisor and generating a signature to identify and prevent similar attacks in the future...").

Moreover, Petitioner's *Capalik* reference is not duplicative of *Kumar* at least

¹⁰ As Petitioner noted above, *Morris* was not cited or considered, based in part on Patent Owner's failure to disclose this reference during prosecution. *Supra*, Introduction. While a distinct 2012 *Morris* publication was cited on the face of the patent, but not considered, the 2007 publication used in Petitioner's challenge herein was never presented to the Office.

because it teaches the allegedly patentable “*wherein the global perspective relates to one or more other events related to the event across a network*” found in each independent claim. Therefore, Petitioner’s cited art differs materially from the prior art substantively considered by the Examiner. Since part one of the *Advanced Bionics* framework is not met, Petitioner need not address part two. *Id.*

B. The General Plastic Factors Favor Institution

Factor 1: Under *General Plastic*, factor 1 considers “whether the same petitioner previously filed a petition directed to the same claims of the same patent.” *See Gen. Plastic Indus. Co. v. Canon Kabushiki Kaisha*, IPR2016-01357, Paper 19, 16 (Sept. 6, 2017) (Section II.B.4.i. precedential). Here, Kaspersky has not previously filed any petition against the ’224 patent.

Kaspersky and the CrowdStrike Petitioners are separate, unrelated petitioners, and are not similarly situated for purposes of Factor 1. Kaspersky was sued separately and accused of infringement based on different products from CrowdStrike. Neither Kaspersky nor the CrowdStrike Petitioners have provided any products or technology to the other leading to an allegation of infringement of the ’224 Patent. This factor weighs in favor of institution and against discretionary denial.

Factors 2, 4, and 5: As to the timing examined in these factors, Kaspersky did not previously file a first petition prior to this petition, and while Kaspersky became aware of the prior art references in the CrowdStrike IPR as of mid-2022, it

made no serial attack on the '224 patent and has filed this IPR within the one-month time period under 37 C.F.R. § 42.122(b). These factors thus weigh in favor of institution and against discretionary denial.

Factor 3: This Petition is Kaspersky's first petition challenging the '224 patent, and Kaspersky has not filed a second petition challenging the same patent. This factor weighs in favor of institution and against discretionary denial.

Factors 6 and 7: These factors weigh in favor of institution, as there should be no material impact on the Board's finite resources or its ability to issue a final determination on CrowdStrike's Petition within one year.

C. The Fintiv Factors Favor Institution

Under the "*Fintiv* factors," the Board may consider parallel litigation, including an early trial date, in determining whether to institute under 35 U.S.C. § 314(a). *NHK Spring Co., Ltd., v. Intri-Plex Technologies, Inc.*, IPR2018-00752, Paper 8 at 19–20 (PTAB Sept. 12, 2018) (precedential); *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 at 2–3, 6 (PTAB Mar. 20, 2020) (precedential). Those factors favor institution here.

1. Stay

Parallel litigation is ongoing. While no stay has been requested, CrowdStrike (one of the defendants in the pending parallel litigation) indicated in the CrowdStrike IPR petition that it will seek a stay of the consolidated litigation if institution is granted. The

CrowdStrike IPR was instituted on May 5, 2023, thus favoring institution. At worst, this factor is neutral because the Board “will not attempt to predict” how the district court will proceed. *Sand Revolution II, LLC v. Continental Intermodal Group-Trucking LLC*, IPR2019-01393, Paper 24 at 7 (PTAB Jun. 16, 2020).

2. Proximity of the Court’s Trial Date

The District Court’s current scheduling order sets the trial date for August 19, 2024, which date is assigned to each defendant in five separate lawsuits that have been consolidated for pretrial issues. *Scheduling Order* (Ex. 1032), 8. Because the court’s consolidation is limited to pretrial issues, separate trials will be required, and trial cannot proceed on August 19, 2024, for all five defendants.

The Board’s FWD deadline in this case is no later than May 2024, three months **before** the currently scheduled trial date. Further, “additional supporting factors” are at play weighing towards a longer than average filing-to-trial window. First, the Kaspersky District Court litigation involves fourteen patents, including ten asserted by Patent Owner against Petitioner and four counterclaim infringement allegations brought by Petitioner. There are six additional patents asserted by Patent Owner against the other defendants. Likewise, the non-Kaspersky defendants have asserted more than a dozen additional counterclaim infringement allegations against Patent Owner. To accommodate the significant number of allegations, the Court has scheduled three Markman hearings. *Id.*, 3, 5, 6. Accordingly, with multiple Markman

hearings, a multitude of claims, and an inability to hold five trials at the same time, the “actual trial date” is more likely to be delayed past the scheduled August 19, 2024, trial date and after FWD here.

In sum, the Board’s FWD deadline in this case falls many months **before** a trial would occur based on the court’s scheduling order. But the additional complicating factors at issue here suggest trial will occur even later in time than the scheduling order sets forth, weighing heavily in favor of institution.

3. Investment in Parallel Proceeding

As indicated above, the parallel proceeding is in its early stages. While the first two Markman hearings have been held, the third is not scheduled until June 13, 2023. Fact discovery opened on April 18, 2023, and is not scheduled to close until January 18, 2024. The deadline to add parties is not until October 3, 2023. Opening expert reports are not due until January 30, 2024, and expert discovery does not close until March 12, 2024. Therefore, the parties have invested minimal time in the parallel proceeding. The lack of investment weighs in favor of institution or is at least neutral.

4. Overlap

Petitioner has raised Capalik and Morris in preliminary invalidity contentions filed in the parallel litigation. However, final infringement and invalidity contentions are not due until October 17, 2023. Therefore, the extent of overlap is unknown at

this time. Further, the Petitioner reserves the right to stipulate to elimination of the overlap between this proceeding and the parallel litigation should the Board allow joinder of this petition with the already instituted CrowdStrike IPR. This would mitigate the concerns over duplication. *Sotera Wireless, Inc. v. Masimo Corp.*, IPR2020-01019, Paper 12, at 18-19 (PTAB Dec. 1, 2020); *SandRevolution II, LLC v. Cont'l Intermodal Group-Trucking LLC*, IPR2019-01393, Paper 24, at 11-12, (PTAB June 16, 2020). Further, the request for institution of the IPR involves additional claims 5, 7, 8, 13, 15, and 16 that are not asserted in the parallel proceeding. Therefore, this factor weighs in favor of institution.

5. Same Party

The Parties are the same in the district court litigation. However, members of the Board have noted *Fintiv* addresses only the scenario in which the petitioner is unrelated to a defendant in a parallel proceeding, finding this should weigh against denying institution, but that *Fintiv* “says nothing about situations in which the petitioner is the same as, or is related to, the district court defendant.” *Cisco Sys., Inc. v. Ramot at Tel Aviv Univ. Ltd.*, IPR2020-00122, Paper 15 at 10-11 (PTAB May 15, 2020) (APJ Crumbley, dissenting) (noting that disfavoring a “defendant in the district court” is “contrary to the goal of providing district court litigants an alternative venue to resolve questions of patentability”). Therefore, this factor weighs slightly against institution.

6. Other Circumstances

“[W]here the PTAB determines that the information presented at the institution stage presents a compelling unpatentability challenge, **that determination alone** demonstrates that the PTAB should not discretionarily deny institution under *Fintiv*.” *Hewlett Packard Enterprise Co., et al. v. Billjco LLC*, IPR2022-00420, Paper 17, at 6 (PTAB July 12, 2022) (“[c]ompelling, meritorious challenges are those in which the evidence, if unrebutted in trial, would plainly lead to a conclusion that one or more claims are unpatentable by a preponderance of the evidence.”). The strength of Petitioner’s proposed grounds presented above weighs strongly in favor of institution. *Id.* (refusing to deny institution under the *Fintiv* framework based solely on the strength of Petitioner’s grounds).

VI. CONCLUSION

For the foregoing reasons, Petitioner respectfully requests *inter partes* review of the Challenged Claims. Petitioner requests their Petition be instituted and joined pursuant to 35 U.S.C. § 315(c) and 37 C.F.R. §§ 42.22 and 42.122(b) with IPR2023-00126, which was instituted May 5, 2023.

Dated: June 2, 2023

Respectfully submitted,

By: /Joseph T. Miotke/
Joseph T. Miotke, Reg. No. 47,798
Dewitt LLP
901 Marquette Avenue
2100 AT&T Tower
Minneapolis, MN 55402
Tel: (612) 305-1400
COUNSEL FOR PETITIONER

VII. MANDATORY NOTICES UNDER 37 C.F.R. § 42.8

A. Real Parties-in-Interest Under 37 C.F.R. § 42.8(b)(1)

The real party-in-interest for this Petition is AO Kaspersky Lab, Petitioner.

B. Related Matters Under 37 C.F.R. § 42.8(b)(2)

The Petitioner is the defendant in a case alleging infringement of the ‘224 patent styled *Webroot, Inc. and Open Text, Inc. v. AO Kaspersky Lab* (Case No. 6:22-CV-00243-ADA-DTG), pending in the Western District of Texas, Waco Division.

The Petitioner further understands that the ‘224 patent has been asserted in the following matters, which matters have been consolidated only for pre-trial purposes with the above matter: *Webroot, Inc. and Open Text, Inc. v. Trend Micro, Inc.* (Case No. 6:22-CV-00239-ADA-DTG); *Webroot, Inc. and Open Text, Inc. v. Sophos Ltd.* (Case No. 6:22-CV-00240-ADA-DTG); and *Webroot, Inc. and Open Text, Inc. v. CrowdStrike, Inc. and CrowdStrike Holdings, Inc.* (Case No. 6:22-CV-00241-ADA-DTG). Each of the four cases will be tried separately.

Finally, the Petitioner understands that the ‘224 patent is the subject of the following IPR petitions: *CrowdStrike, Inc. v. Webroot, Inc.* in IPR2023-00126 and *Trend Micro Inc. v. Open Text, Inc.* in IPR2023-00657. Petitioners request their Petition be instituted and joined pursuant to 35 U.S.C. § 315(c) and 37 C.F.R. §§ 42.22 and 42.122(b) with IPR2023-00126, which was instituted May 5, 2023.

C. Lead and Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3)

Petitioner designates Joseph T. Miotke (Reg. No. 47,798) as lead counsel and Eric Chadwick (Reg. No. 41,664), and Erin Block (Reg. No. 78,154) as back-up counsel.

Service of any documents may be made at the postal mailing address of Dewitt LLP, 901 Marquette Ave., 2100 AT&T Tower, Minneapolis, MN 55402, (Tel: (612) 305-1400 and Fax: (612) 305-1414).

Petitioner consents to electronic service by email to the email addresses:

jtm@dewittllp.com;

ehc@dewittllp.com;

eblock@dewittllp.com; and

docketing@dewittllp.com.

APPENDIX OF EXHIBITS

Exhibit 1001	U.S. Patent No. 10,257,224 to Jaroch et al.
Exhibit 1002	File History of U.S. Patent No. 10,257,224
Exhibit 1003	Declaration of Dr. Wenke Lee
Exhibit 1004	U.S. Publication No. 2013/0298244 to Kumar et al.
Exhibit 1005	U.S. Publication No. 2007/0016953 to Morris et al. (“ <i>Morris</i> ”)
Exhibit 1006	U.S. Patent No. 8,087,087 to Van Oorschot et al. (“ <i>Van Oorschot</i> ”)
Exhibit 1007	U.S. Publication No. 2010/0077481 to Polyakov et al.
Exhibit 1008	U.S. Publication No. 2011/0321166 to Capalik et al. (“ <i>Capalik</i> ”)
Exhibit 1009	U.S. Publication No. 2012/0260340
Exhibit 1010	File History of U.S. Patent No. 9,578,045 (“’045 Patent File History”)
Exhibit 1011	Scheduling Order (Dkt. 50)
Exhibit 1012	Natarajan Meghanathan, Sumanth Reddy Allam, and Loretta A. Moore, <i>Tools and Techniques for Network Forensics</i> , International Journal of Network Security & Its Applications (IJNSA), Vol. 1., No. 1 (April 2009)
Exhibit 1013	SANS Institute, <i>Host- vs. Network-Based Intrusion Detection Systems</i> (2000-2005)
Exhibit 1014	Securosis LLC, <i>Evolving Endpoint Malware Detection: Dealing with Advanced and Targeted Attacks</i> , Version 1.3 (July 12, 2012)
Exhibit 1015	Yanfang Ye, Weiwei Zhuang, Tao Li, Egemen Tas, Umesh Gupta, Shenghuo Zhu, Melih Abdulhayogiu, <i>Combining File Content and File Relations for Cloud Based Malware Detection</i> (August 2011)
Exhibit 1016	U.S. Patent No. 6,944,772 to Dozortsev
Exhibit 1017	U.S. Patent No. 6,772,346 to Chess et al.
Exhibit 1018	WO 2002/033525 to Shyne-Song Chuang
Exhibit 1019	EP 1,549,012 to Kristof De Spiegeleer
Exhibit 1020	EP 1,280,040 to Alexander James Hinchliffe et al.
Exhibit 1021	Oracle, Java Documentation, <i>The Java Tutorials, What is a Path? (And Other File System Facts)</i> (available at the following link https://docs.oracle.com/javase/tutorial/essential/io/path.html) (last accessed October 2022)
Exhibit 1022	U.S. Patent Publication No. 2004/0143753 to Hernacki et al.
Exhibit 1023	U.S. Patent Publication No. 2011/0083180 to Mashevsky et al.
Exhibit 1024	U.S. Patent No. 8,429,746 to Alen Capalik

Exhibit 1025	<i>Server Hardware, Software and Architecture</i> by Abeer El Hadi El Zein El Nahas, University of Khartoum, Electrical and Electronics Engineering Dept. (Feb. 2008)
Exhibit 1026	Guofei Gu, Phillip Porras, Vinod Yegneswaran, Martin Fong, Wenke Lee, <i>BotHunter: Detecting Malware Infection Through IDS-Driven Dialog Correlation</i> , In Proceedings of The 16th USENIX Security Symposium (August 2007)
Exhibit 1027	Yacin Nadji, Manos Antonakakis, Roberto Perdisci, and Wenke Lee, <i>Understanding the Prevalence and Use of Alternative Plans in Malware with Network Games</i> , In Proceedings of The 27th Annual Computer Security Applications Conference (December 2011)
Exhibit 1028	Manos Antonakakis, Roberto Perdisci, David Dagon, Wenke Lee, and Nick Feamster, <i>Building a Dynamic Reputation System for DNS</i> , In Proceedings of The 19th USENIX Security Symposium, (August 2010)
Exhibit 1029	Long Lu, Vinod Yegneswaran, Phil Porras, and Wenke Lee, <i>BLADE: An Attack-Agnostic Approach for Preventing Drive-By Malware Infections</i> , In Proceedings of The 17th ACM Conference on Computer and Communications Security (CCS), Chicago, IL (October 2010)
Exhibit 1030	U.S. Publication No. 2008/0016570 to Capalik
Exhibit 1031	Declaration of V.S. Subrahmanian, Ph.D.
Exhibit 1032	Order Granting Fifth Amended Scheduling Order, ECF No. 252, Mar. 29, 2023

CLAIM LISTING APPENDIX

U.S. Patent No. 10,257,224, Claims 1-4, 7-8, 10-13, and 16-19

Claim Designation	Claim Language
Claim 1[P]	A method comprising:
Claim [1(a)]	gathering an event defining an action of a first object acting on a target,
Claim [1(a)(i)]	wherein the first object is executed on a device;
Claim [1(b)]	generating contextual state information for the event by correlating the event to an originating object of the first object;
Claim [1(c)]	obtaining a global perspective for the event based on the contextual state information,
Claim [1(c)(i)]	wherein the global perspective comprises information associated with one or more of the first object and the originating object,
Claim [1(c)(ii)]	and wherein the global perspective relates to one or more other events related to the event across a network;
Claim [1(d)]	generating an event line comprising information relating to the event,
Claim [1(d)(i)]	wherein the information relates to at least one of the first object, the action of the first object, the target, and the originating object; and
Claim [1(e)]	transmitting the generated event line.
Claim 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.
Claim 3	The method of claim 1, further comprising: obtaining an event priority based on one or more of the generated contextual state information and the global perspective, wherein the event line further includes the event priority.
Claim 4	The method of claim 1, wherein the event includes information identifying the first object performing the action, information identifying the action being performed, and information identifying the target upon which the act is being performed.

Claim 7	The method of claim 4, further comprising: heuristically displaying the information identifying the first object performing the action, the information identifying the action being performed, the information identifying the target upon which the act is being performed, and information associated with the global perspective according to one or more of: a location associated with the first object; at least one characteristic of an outbound connection associated with the first object; a dropped executable file; an age of the first object; and a number of concurrent connections associated with the first object.
Claim 8	The method of claim 1, wherein the global perspective comprises information comprises at least one of: an age; a popularity; a determination as to whether the first object is malware; a determination as to whether the originating object is malware; an Internet Protocol (IP) Address; and a Uniform Resource Locator (URL).
Claim 10[P]	A system for providing forensic visibility into a system, comprising:
Claim [10(a)]	a device comprising:
Claim [10(b)]	a communication interface;
Claim [10(c)]	a processor;
Claim [10(d)]	data storage; and
Claim [10(e)]	a sensor agent stored on the data storage that is executable by the processor, wherein the sensor agent is operable to:
Claim [10(e)(i)]	gather an event defining an action of a first object acting on a target;
Claim [10(e)(ii)]	generate contextual state information for the event by correlating the event to an originating object of the first object;
Claim [10(e)(iii)]	obtain a global perspective for the event based on the contextual state information,
Claim [10(e)(iv)]	wherein the global perspective comprises information associated with one or more of the first object and the originating object,
Claim [10(e)(v)]	and wherein the global perspective relates to one or more other events related to the event across a network;
Claim [10(e)(vi)]	generate an event line comprising information relating to the event,
Claim [10(e)(vii)]	wherein the information relates to at least one of the first object, the action of the first object, the target, and the originating object; and

Claim [10(e)(viii)]	transmit the generated event line utilizing the communication interface.
Claim 11	The system of claim 10, wherein the event is executed by the processor.
Claim 12	The system of claim 10, further comprising: a global perspective information server; and an end recipient device, wherein the information associated with the one or more of the first object and the originating object is obtained from the global perspective information server and the sensor agent transmits the event line to the end recipient device.
Claim 13	The system of claim 10, wherein the event includes information identifying the first object performing the action, information identifying the action being performed, and information identifying the target upon which the act is being performed.
Claim 16	The system of claim 13, wherein the end recipient device heuristically displays the information identifying the first object performing the action, the information identifying the action being performed, the information identifying the target upon which the act is being performed, and information associated with the global perspective according to one or more of: a location associated with the first object; at least one characteristic of an outbound connection associated with the first object; a dropped executable file; an age of the first object; and a number of concurrent connections associated with the first object.
Claim 17[P]	A system for providing forensic visibility into a system, comprising:
Claim [17(a)]	a first device comprising:
Claim [17(b)]	a communication interface;
Claim [17(c)]	a processor;
Claim [17(d)]	data storage; and
Claim [17(e)]	a sensor agent stored on the data storage that is executable by the processor, wherein the sensor agent is operable to:
Claim [17(e)(i)]	gather an event defining an action of a first object acting on a target;
Claim [17(e)(ii)]	determine a global perspective for the event based on contextual state information for the event,
Claim [17(e)(iii)]	wherein the global perspective relates to one or more other events related to the event across a network, and

Claim [17(e)(iv)]	wherein the contextual state comprises an indication of an originating object of the first object and an indication of at least one of a second device on which the first object is executed and a user associated with the first object;
Claim [17(e)(v)]	generate an event line comprising information relating to the event,
Claim [17(e)(vi)]	wherein the information relates to at least one of the first object, the action of the first object, the target, and the originating object; and
Claim 17(e)(vii)]	transmit the generated event line utilizing the communication interface.
Claim 18	The system of claim 17, further comprising a global perspective information server comprising: a processor; a communication interface; data storage; and a global perspective module, wherein the global perspective module is operable to: receive the event line from the device; assemble a second event line including details associated with the event, wherein the second event line comprises information identifying the first object, information identifying the action of the first object, information identifying the target, and information identifying the originating object; and transmit the second event line utilizing the communication interface to an end recipient.
Claim 19	The system of claim 18, wherein the end recipient heuristically displays the information identifying the first object, the information identifying the action of the first object, the information identifying the target, and information associated with the global perspective according to one or more of: a location associated with the first object; at least one characteristic of an outbound connection associated with the first object; a dropped executable file; an age of the first object; and a number of concurrent connections associated with the first object.

CERTIFICATE OF COMPLIANCE UNDER 37 C.F.R. § 42.24(d)

Pursuant to 37 C.F.R. § 42.24(d), Petitioner hereby certifies, in accordance with and reliance on the word count provided by the word-processing system used to prepare this Petition, that the number of words in this paper is 13,994. Pursuant to 37 C.F.R. § 42.24(d), this word count excludes the table of contents, mandatory notices under § 42.8, certificate of service, certificate of word count, appendix of exhibits, and any claim listing.

Dated: June 2, 2023

Respectfully submitted,

By: /Joseph T. Miotke/
Joseph T. Miotke, Reg. No. 47,798
Dewitt LLP
901 Marquette Avenue
2100 AT&T Tower
Minneapolis, MN 55402
Tel: (612) 305-1400
COUNSEL FOR PETITIONER

CERTIFICATE OF SERVICE

The undersigned certifies that, in accordance with 37 C.F.R. § 42.6(e) and 37 C.F.R. § 42.105, service was made on Patent Owner as detailed below.

Date of service June 2, 2023

Manner of service FEDERAL EXPRESS

Documents served Petition for Joinder; Petition for *Inter Partes* Review

Under 35 U.S.C. § 312 and 37 C.F.R. § 42.104 of U.S.
10,284,591; Petitioner's Exhibit List; Exhibits 1001-
1032; and Petitioner's power of attorney.

Persons served Sprinkle IP Law Group
1301 W. 25th Street, Suite 400
Austin, TX 78705

Dated: June 2, 2023

Respectfully submitted,

By: /Joseph T. Miotke/
Joseph T. Miotke, Reg. No. 47,798
Dewitt LLP
901 Marquette Avenue
2100 AT&T Tower
Minneapolis, MN 55402
Tel: (612) 305-1400
COUNSEL FOR PETITIONER