

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CROWDSTRIKE, INC.

Petitioner

v.

OPEN TEXT INC.

Patent Owner

Case IPR2023-00124

Patent No. 9,578,045

**DECLARATION OF PROFESSOR NENAD MEDVIDOVIC, Ph.D.
IN SUPPORT OF PATENT OWNER**

TABLE OF CONTENTS

I.	QUALIFICATIONS	2
II.	UNDERSTANDING OF RELEVANT LEGAL PRINCIPLES	7
III.	STATE OF THE PRIOR ART	9
IV.	The '045 Patent.....	10
	A. Summary Of The '045 Patent.....	10
	B. Claim Construction.....	16
	C. Level of Ordinary Skill In The Art	18
V.	PETITIONER’S GROUND 1 DOES NOT DISCLOSE OR RENDER OBVIOUS THE CHALLENGED CLAIMS.....	19
	A. Overview Of Morris	20
	B. Independent Claims 1, 8, And 16.....	21
	1. Morris Does Not Disclose Or Render Obvious Limitations [1(b)], [8(e)(ii)], and [16(g)(i)].....	21
	2. The USPTO’s Allowance of the '224 Continuation Patent Further Supports My Opinion.....	26
	C. Dependent Claims	27
VI.	PETITIONER’S GROUND 2 DOES NOT DISCLOSE OR RENDER OBVIOUS THE CHALLENGED CLAIMS.....	27
	A. Overview Of Capalik.....	27
	B. Independent Claims 1, 8, And 16	31
	1. Capalik Does Not Disclose Or Render Obvious Limitations [1(c)(ii)], [10(e)(v)], And [17(e)(iii)]	31
	2. The USPTO’s Allowance Of The '224 Continuation Patent Further Supports My Opinion.....	36

C.	Dependent Claims	37
VII.	CLAIMS AND/OR LIMITATIONS NOT ADDRESSED IN THIS DECLARATION	37
VIII.	SECONDARY OBJECTIVE INDICIA OF NONOBVIOUSNESS	38
IX.	CONCLUSION.....	39

EXHIBIT LIST

Exhibit	Description
2001	Declaration of Professor Nenad Medvidovic, Ph.D
2002	<i>Curriculum Vitae</i> of Professor Nenad Medvidovic, Ph.D.
2003	<i>Webroot, Inc. and Open Text Inc., v. CrowdStrike, Inc. and CrowdStrike Holdings, Inc.</i> , Case No. 6:22-cv-00241-ADA-DTG, First Amended Complaint for Patent Infringement, Dkt. 60 (W.D. Tex., Sept. 8, 2022) (excerpted)
2004	<i>Sonrai Memory Ltd. v. Kingston Tech. Co. and Kingston Tech. Corp.</i> , Case No. 6:21-cv-1284-ADA, Order Denying Kingston Tech. Co. and Kingston Tech. Corp.’s Opposed Motion to Stay Pending Resolution of <i>Inter Partes</i> Review, Dkt. 94 (W.D. Tex., Oct. 18, 2022)
2005	<i>mCom IP, LLC v. Cisco Systems, Inc.</i> , Case No. 6:22-cv-00261-ADA, Order Denying Defendant’s Motion to Stay Pending <i>Inter Partes</i> Review, Dkt. 42 (W.D. Tex., Oct. 20, 2022)
2006	<i>Intellectual Ventures I LLC et al. v. Hewlett Packard Enterprise Co.</i> , No. 6:21-cv-00596-ADA, Order Denying Hewlett Packard Enterprise Company’s Opposed Motion to Stay Pending Resolution of <i>Inter Partes</i> Review, Dkt. 104 (W.D. Tex., Dec. 22, 2022)
2007	<i>Webroot, Inc., Open Text Inc., v. AO Kaspersky Lab et al.</i> , Case No. 6:22-cv-00243-ADA-DTG, Order Granting Third Amended Scheduling Order, Dkt. 142 (W.D. Tex., Dec. 27, 2022)
2008	<i>Webroot, Inc. and Open Text Inc., v. AO Kaspersky Lab. et al.</i> , Case No. 6:22-cv-243-ADA-DTG, Claim Construction Order, Dkt. 236 (W.D. Tex. Mar. 16, 2023)
2009	<i>Webroot, Inc. and Open Text Inc., v. AO Kaspersky Lab et al.</i> , Case No. 6:22-cv-00243-ADA-DTG, Defendants’ Opening Claim Construction Brief, Dkt. 86 (W.D. Tex., Oct. 28, 2022) (excerpted)

Exhibit	Description
2010	<i>Webroot, Inc. and Open Text Inc., v. AO Kaspersky Lab et al.</i> , Case No. 6:22-cv-00243-ADA-DTG, Defendants’ Reply Claim Construction Brief, Dkt. 110 (W.D. Tex., Dec. 6, 2022) (excerpted)
2011	<i>Webroot, Inc. and Open Text Inc., v. AO Kaspersky Lab et al.</i> , Case No. 6:22-cv-00243-ADA-DTG, Scheduling Order, Dkt. 50 (W.D. Tex., Sept. 28, 2022) (excerpted)
2012	<i>Open Text Inc. et al., v. AO Kaspersky Lab</i> , Case No. 6:22-cv-00243-ADA-DTG, Defendant AO Kaspersky Lab’s Preliminary Invalidity Contentions Exhibit 4A (W.D. Tex., Sept. 14, 2022) (excerpted)
2013	<i>Webroot, Inc. and Open Text Inc., v. Sophos Ltd.</i> , Case No. 6:22-cv-00240-ADA-DTG, Defendant Sophos Ltd.’s Preliminary Invalidity Contentions (W.D. Tex., Sept. 13, 2022) (excerpted)
2014	<i>Webroot, Inc. and Open Text Inc., v. Trend Micro Inc.</i> , Case No. 6:22-cv-00239-ADA-DTG, Defendant’s Preliminary Invalidity Contentions (W.D. Tex., Sept. 13, 2022) (excerpted)
2015	<i>Webroot, Inc. and Open Text Inc., v. CrowdStrike, Inc. and CrowdStrike Holdings, Inc.</i> , Case No. 6:22-cv-00241-ADA, Complaint for Patent Infringement, Dkt. 1 (W.D. Tex., Mar. 4, 2022)
2016	<i>Open Text Inc. et al., v. AO Kaspersky Lab</i> , Case No. 6:22-cv-00243-ADA-DTG, First Amended Complaint for Patent Infringement, Dkt. 80 (W.D. Tex., Oct. 27, 2022)
2017	<i>Webroot, Inc. and Open Text Inc., v. Trend Micro Inc.</i> , Case No. 6:22-cv-00239-ADA-DTG, First Amended Complaint for Patent Infringement, Dkt. 53 (W.D. Tex., Sept. 7, 2022)
2018	<i>Webroot, Inc. and Open Text Inc., v. Sophos, Ltd.</i> , Case No. 6:22-cv-00240-ADA-DTG, Second Amended Complaint for Patent Infringement, Dkt. 76 (W.D. Tex., Oct. 24, 2022)
2019	File History for Continuation Patent, U.S. Patent No. 10,257,224

Exhibit	Description
2020	U.S. Patent Application Publication No. 2008/0016570 to Capalik (“Capalik 570”)
2021	<i>Webroot, Inc. and Open Text Inc., v. AO Kaspersky Lab. et al.</i> , Case No. 6:22-cv-243-ADA-DTG, March 9, 2022 Transcript of Motions Hearing, Dkt. 133 (W.D. Tex. Dec. 15, 2022) (excerpted)
2022	U.S. Patent No. 10, 257,224 to Joseph Jaroch (“’224 Patent”)
2023	Joseph Jaroch LinkedIn

I, Professor Nenad Medvidovic, Ph.D., declare as follows:

1. I have been engaged by King & Spalding LLP on behalf of OpenText Inc. (“Patent Owner”), to provide this Declaration concerning the technical subject matter relevant to the petition for Inter Partes Review (“Petition”) of U.S. Patent 9,578,045 (“the ’045 patent”).

2. I am over 18 years of age. I have personal knowledge of the facts stated in this Declaration and could testify competently to them if asked to do so.

3. I have reviewed and am familiar with the specification and the claims of the ’045 patent. In general, I will cite to the specification of a United States patent using the following formats: (Exhibit No. Col:Line Number(s)) or (Exhibit No. Paragraph Number(s)). For example, the citation (EX-1001 1:1–10) points to the ’045 patent specification at column 1, lines 1–10. Also, for convenience, I use italics to denote limitations from the challenged claims.

4. All the opinions in this Declaration are based on the documents I reviewed and my knowledge and professional judgment. In forming the opinions expressed in this Declaration, I reviewed the Petition for *Inter Partes* Review of U.S. Patent No. 9,578,045 and supporting exhibits.

5. I have been asked to provide my technical opinions regarding how a person of ordinary skill in the art would have understood the claims of the ’045 patent at the time of the alleged invention. I have also been asked to provide my

technical opinions on how concepts in the '045 patent specification relate to claim limitations of the '045 patent. In reaching the opinions provided herein, I have considered the '045 patent, its prosecution history, and the references cited above and have drawn as appropriate on my own education, training, research, knowledge, and personal and professional experience.

I. QUALIFICATIONS

6. In formulating my opinions, I have relied on my knowledge, training, and experience in the relevant field, which I will summarize briefly. A more detailed summary of my background, experience, and publications is set forth in my curriculum vitae (CV), which is submitted as Exhibit 2002.

7. I received a Bachelor of Science degree, Summa Cum Laude, from Arizona State University's Computer Science and Engineering department.

8. I received a Master of Science degree from the University of California at Irvine's Information and Computer Science department.

9. I received a Doctor of Philosophy degree from the University of California at Irvine's Information and Computer Science department. My dissertation was entitled "Architecture-Based Specification-Time Software Evolution."

10. For more than 25 years, my research has focused on the building blocks that comprise software systems: software components (computational and data elements) and connectors (interaction-facilitating elements), and mechanisms for their

implementation, primarily middleware facilities and software frameworks. In particular, my Ph.D. dissertation—whose first research results were published in 1995 while the dissertation was completed in 1999—yielded a new design style for the development and evolution of highly distributed software systems built out of independent components that exchange different types of information encoded in messages in order to accomplish specific goals. This research focused on the design principles behind such systems, the appropriate support for modeling the systems (both at the level of individual agents as well as their integrations into subsystems and entire systems), and the infrastructure for their implementation, deployment, and optimization. This work was applied across a wide range of domains, from traditional distributed systems to mobile devices and autonomous robots.

11. I am employed by the University of Southern California (“USC”) as a faculty member in the Computer Science Department and have been since January 1999. I currently hold the title of Professor with tenure. Since July 2022, I have served as my department’s Chairman. Between January 2009 and January 2013, I served as the Director of the Center for Systems and Software Engineering at USC. Between July 2011 and July 2015, I served as my Department’s Associate Chair for Ph.D. Affairs. Between July 2021 and June 2022, I served as my Department’s Vice-Chair for Tenure Affairs.

12. I teach graduate and undergraduate courses in Software Architecture, Software Engineering, and Embedded Systems, and I advise Ph.D. students. I have graduated 19 Ph.D. students and advise 7 students currently pursuing a Ph.D.

13. I served as Program Co-Chair for the flagship conference in my field—International Conference on Software Engineering (“ICSE”)—held in May 2011. I have served as Chair or Co-Chair for various other conferences in the Software Engineering field, including: the Fifth Working Institute of Electrical and Electronics Engineers (“IEEE”)/IFIP Conference on Software Architecture, the Third IEEE International Conference on Self-Adaptive and Self-Organizing Systems, the Fifteenth International Association for Computing Machinery’s (“ACM”) Special Interest Group on Software Engineering (“SIGSOFT”) Symposium on Component Based Software Engineering, the IEEE/CSSE/ISE Workshop on Software Architecture Challenges for the 21st Century, and the Doctoral Symposia at the Sixteenth ACM SIGSOFT International Symposium on the Foundations of Software Engineering and at the 44th International Conference on Software Engineering.

14. I serve or have served as an editor of several peer-reviewed journals, including: “IEEE Transactions on Software Engineering,” “ACM Transactions on Software Engineering and Methodology,” “Journal of Software Engineering for Robotics,” “Elsevier Information and Software Technology Journal,” “Journal of Systems and Software,” “Journal of Software Engineering Research and Development,”

and “Springer Computing Journal.” Additionally, I have served as a guest editor of several special issues for different journals. Since January 2018, I have served as Editor-in-Chief of “IEEE Transactions on Software Engineering.”

15. Between September 2013 and September 2015, I served as Chair of the ICSE Steering Committee. Both prior to that (2008-2013) and subsequent to that (2015-present) I have been a member of the ICSE Steering committee. I am currently a member of the Steering Committee of the joint European Conference on Software Engineering and the Symposium on the Foundations of Software Engineering (“ESEC/FSE”). From July 2015 to September 2017, I chaired the Steering Committee of FSE, while it was a standalone symposium. I previously served as a member of the Steering Committees of the Working IEEE/IFIP Conference on Software Architecture.

16. Between July 2015 and June 2018, I served as Chair of the ACM SIGSOFT, the largest professional organization in my field of work. During the past year, I have chaired the Committee in charge of ACM’s Software System Award, one of the most important technical awards given in my field.

17. I co-authored “Software Architecture: Foundations, Theory, and Practice,” a widely used textbook in the field of Software Systems’ Architecture.

18. I have served as editor of various books in the Software Engineering field including: “Proceedings of the 3rd International Conference on Self-Adaptive

and Self-Organizing Systems,” “Proceedings of the Warm-Up Workshop for the 32nd International Conference on Software Engineering,” “Proceedings of the 5th Working IEEE/IFIP Conference on Software Architecture,” and “40 Editions of ICSE – The Ruby Anniversary Celebration.”

19. I have authored or co-authored nearly 300 papers in the Software Engineering field. My most cited paper has been cited well over 3,000 times. A paper I co-authored in the 1998 International Conference on Software Engineering, my field’s flagship conference, was given ten years later, in 2008, that conference’s Most Influential Paper Award. Another one of my publications received a Most Influential Paper Award in 2020. Several of my other publications have received “best paper” or “most cited” awards.”

20. Several of my publications have focused on different aspects of computer security. A paper describing a security-vulnerability detection tool for Android devices, built in my lab, won the Best Tool Paper award at the 2017 Automated Software Engineering Conference. I have co-authored three patents in the area of cybersecurity.

21. I have been named a Distinguished Scientist of the ACM. I have been elected a Fellow of the IEEE, IEEE’s highest grade that is granted to less than 0.1% of its membership annually.

II. UNDERSTANDING OF RELEVANT LEGAL PRINCIPLES

22. I am not a lawyer, and I will not provide any legal opinions. Although I am not a lawyer, I have been advised certain legal standards are to be applied by technical experts in forming opinions regarding the meaning and validity of patent claims.

23. I understand that a patent claim is invalid if it is anticipated or obvious in view of the prior art, and that a claim can be unpatentable even if all of the requirements of the claim cannot be found in a single prior-art reference. I further understand that invalidity of a claim requires that the claim be anticipated or obvious from the perspective of a person of ordinary skill in the art at the time the invention was made.

24. I have been informed that a patent claim is invalid if it would have been obvious to a person of ordinary skill in the art. In analyzing the obviousness of a claim, I understand the following factors may be taken into account: (1) the scope and content of the prior art; (2) the differences between the prior art and the claims; (3) the level of ordinary skill in the art; and (4) any so called “secondary considerations” of nonobviousness if they are present.

25. I have been informed that a claim can be obvious in light of a single prior art reference or multiple prior art references. I understand that to prove that prior art or a combination of prior art renders a patent obvious, it is necessary to:

- 1) Identify the particular references that, singly or in combination, make the patent obvious;
- 2) Specifically identify which elements of the patent claim appear in each of the asserted references; and
- 3) Explain why a person of ordinary skill in the art would have combined the references, and how they would have done so, to create the inventions claimed in the patent. I further understand that exemplary rationales that may support a conclusion of obviousness include:
 - Combining prior art elements according to known methods to yield predictable results;
 - Simple substitution of known element for another to obtain predictable results;
 - Use of known technique(s) to improve similar devices (methods or products) in the same way;
 - Applying a known technique to a known device (method or product) ready for improvement to yield predictable results;
 - “Obvious to try” – choosing from a finite number of identified, predictable solutions with a reasonable expectation of success;
 - Known work in one field of endeavor may prompt variations of the work for use in either the same field or a different field based on design incentives or other market forces if the variations are predictable to a person of ordinary skill in the art; and
 - Some teaching, suggestion, or motivation in the prior art that would have led a person of ordinary skill in the art to modify the prior art reference or

to combine the prior art reference teachings to arrive at the claimed invention.

26. I have been informed that, in considering obviousness, hindsight reasoning derived from the patent-at-issue may not be used.

III. STATE OF THE PRIOR ART

27. Network forensics generally relates to intercepting and analyzing network events to discover the source of security attacks. (EX-1001 1:22-24.) At the time of invention of the '045 patent, network forensics systems used network forensics tools, *e.g.*, network sniffers and packet capture tools, to detect and capture information associated with communication sessions. (*See* EX-1001 1:24-33.) Although such network forensics tools passively collect network traffic, the tools resided at a network edge, *e.g.*, one or more locations where an organization's network interfaces with the Internet. (*See* EX-1001 1:33-43.) That is, a network forensics tool, such as a network sniffer, may reside at a network edge and may receive network events concerning the network from one or most hosts or systems, but network edge devices have no ability to establish any sort of context from within the host or system that is generating the event. (*See* EX-1001 1:40-46.)

28. As a result, the network forensics tools could not obtain useful information within a host or establish any sort of context from within a host that was generating and/or receiving network events. (*See* EX-1001 3:49-52.) Without this

information, prior art network forensics tools were insufficient to identify and address the threats faced by modern computer networks. (*See* EX-1001 1:46-49.) Although a network edge device could monitor, capture, and analyze communications traffic, the network edge device could not provide details regarding files modified, registry entry changes, or new processes created within the network core. (*See* EX-1001 1:63-2:12.) The network edge device thus had no way of knowing to what extent a virus may have impacted the computing device, what additional files may have become infected, or what processes and/or objects operating are linked to the virus. (*See* EX-1001 2:12-16.)

29. Accordingly, there was a long-felt need for a solution that eliminated the guesswork by allowing for end-to-end visibility of events within a system and/or within a network. (EX-1001 2:16-19.)

IV. THE '045 PATENT

A. Summary Of The '045 Patent

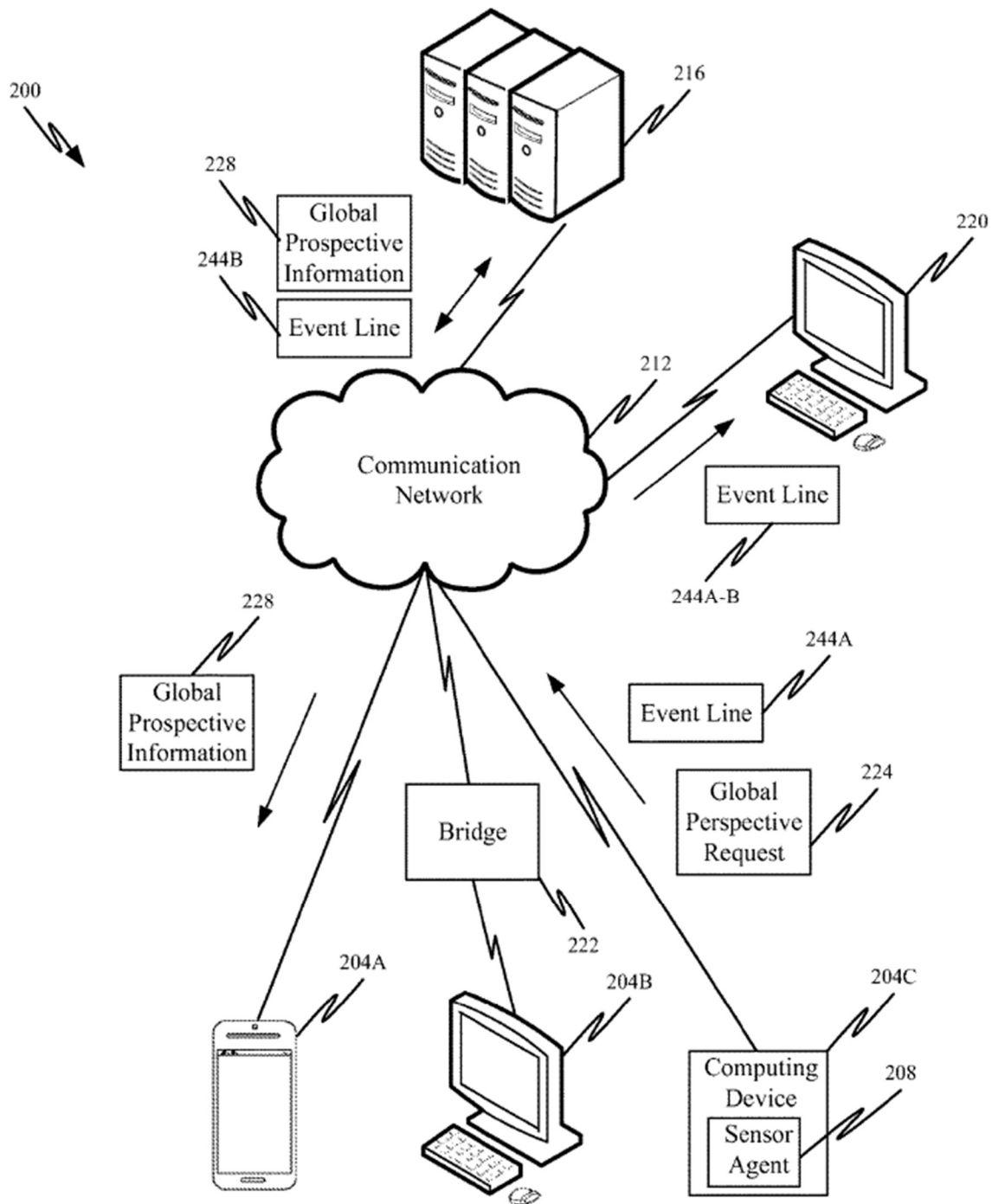
30. The '045 Patent is entitled “Method and Apparatus for Providing Forensic Visibility into Systems and Networks” and describes and claims a system and method that significantly improved on the traditional network forensics tools used to discover or identify security issues on computer networks. (EX-1001 Abstract, 2:36-38.)

31. Unlike traditional network forensics tools, the '045 Patent creates forensic visibility into the computing devices on the communication network to identify malware or other security issues in operation of those devices. (EX-1001 2:38–40.) The described and claimed systems and methods intercept network “events,” create audit trails for each individual event by correlating the event to “objects” such as their originating processes, devices, and/or users, and establish a global perspective of the objects. “Events may define those actions or behaviors of an object acting upon another object or some other entity.” (EX-1001 7:31-32.) An “object” may include “a computer file, part of a file or a sub-program, macro, web page or any other piece of code to be operated by or on the computer, or any other event whether executed, emulated, simulated or interpreted.” (EX-1001 7:32-36.)

32. This system and method for analyzing the behavior of objects to identify those that are potentially malicious further improves malware detection by understanding the context of the event and computer objects of interest. (EX-1001 2:39-43 (“The system filters may be built upon the same or similar technology related to behavior monitoring and collection, as discussed in U.S. Application Ser. No. 13/372,375 filed Feb. 13, 2012, ‘Method and Apparatus for Dealing with Malware.’”) (incorporating Morris 340 “in its entirety for all that it teaches and for all purposes.”).) In many cases, a potentially malicious object is identified by the

system as a result of other events that provide information as to whether the code is malicious.

33. In particular, the '045 Patent improves network security by gathering an “event,” generating “contextual state information,” obtaining a “global perspective” for the event, and generating and transmitting an “event line” that includes information for the event. (*See* EX-1001 cl. 1.) Figure 2, below, illustrates an exemplary communication network having one or more end recipients, *e.g.*, computing devices 204A-C, and a global perspective information server 216:



(EX-1001 Fig. 2, 6:46-62.)

34. A computing device may include and/or execute a sensor agent 208 (which may be made up of multiple modules) to gather and process events. (EX-

1001 7:9-14.) In one embodiment, contextual state information is generated by correlating events to objects and may include originating processes, devices, and users. (*Id.* 8:30-32, 8:42-43; *see also, e.g.*, cl. 1.) “[T]he originating process or object may [be] determined based on a previous event that initiated or otherwise created the current process and/or object.” (*Id.* 17:39-42.)

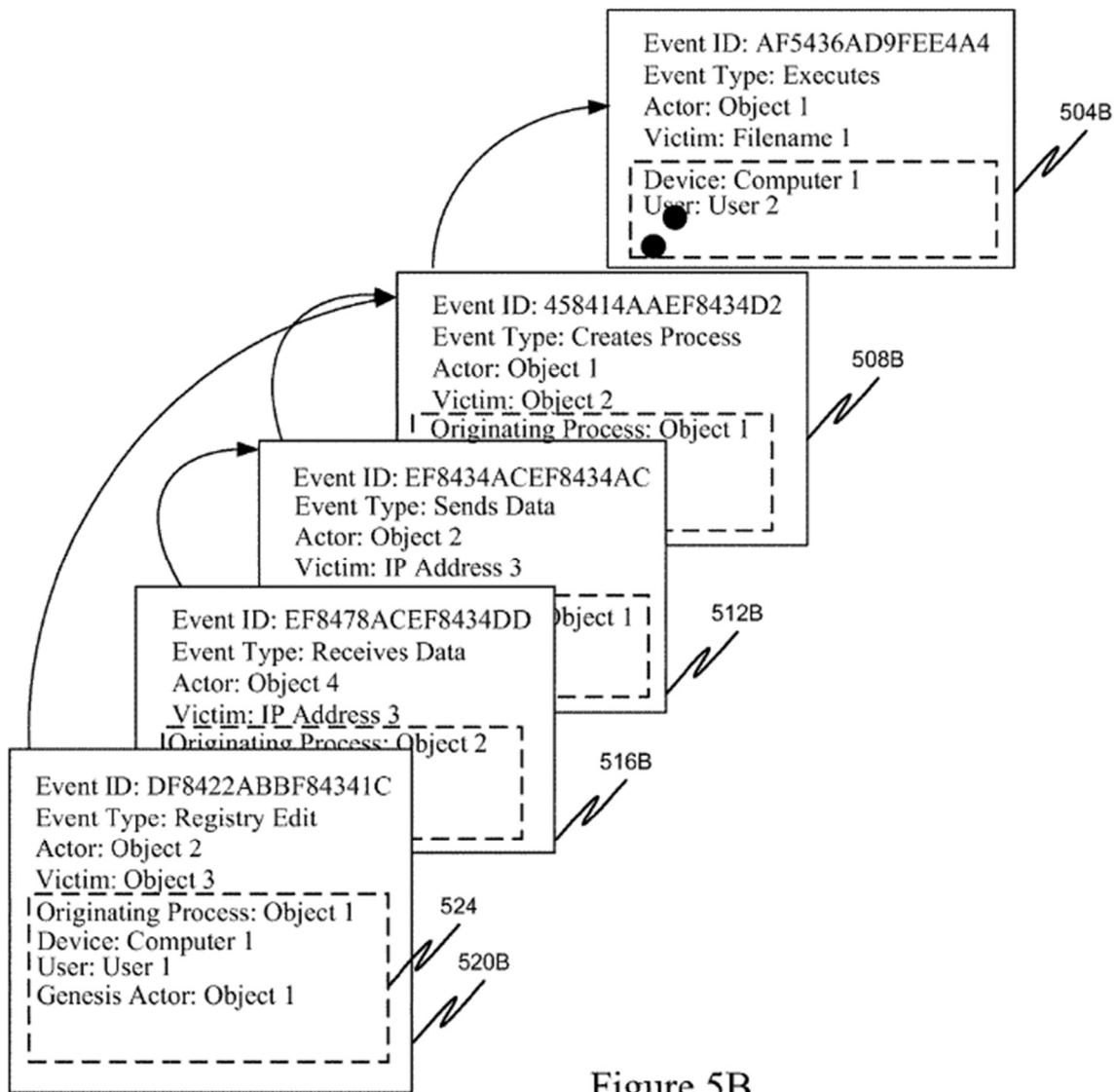


Figure 5B

35. In another embodiment, contextual state information may additionally include “GenesisActor information,” which “may contain the object that is not the

direct Actor of an event but which is the ultimate parent of the event being performed.” (EX-1001 8:45-51.) “For example in the case of a software installation, the GenesisActor would be the object that the user or system first executed and that initiated the software installation process, e.g. Setup.exe.” (*Id.* 8:48-51.) Figure 5B illustrates a context 520B as comprising an originating process, GenesisActor, device, and user; however, “the contextual information forming the contextual state 520B may include more or less information and in varying combinations.” (*Id.* 17:35-38.)

36. A sensor agent may obtain a global perspective for each event—for example, by calling on the global perspective information server or determining if the information is available locally within a cache. (EX-1001 9:4-9.) Global perspective information “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.* 9:19-22.) The combination of contextual information and global perspective enables detection of new zero-day threats, including objects created from objects (or similar objects) that have been identified previously as malicious. As malicious code and threats evolve more quickly, this combined approach improves detection time and enhances overall network security.

37. An event line is assembled or generated, containing information from and/or regarding the event, and may be transmitted to other devices. (EX-1001 9:50-

10:18.) The generation of the event line makes it easier for end users to “identify events, and/or instances of malware, that require more immediate attention”—thereby improving the accuracy and efficiency of identifying additional malicious code, as well as enabling administrators to more readily analyze malware, assess vulnerabilities, and correct damage done by the originating objects. (EX-1001 9:45-49.)

38. Thus, the '045 Patent describes and claims systems and methods that provide more efficient and accurate identification of malware and which improved the identification of other malware (and corresponding event(s)) that might otherwise go undetected in prior systems. This improved system performance and reduced the number of resources required.

B. Claim Construction

39. Petitioner does not construe claim terms in its Petition.

40. In the parallel district court litigation, the Court construed the following terms—all of which are present in the claims challenged by Petitioner in its petition—in its March 16, 2023 claim construction order (EX-2008), which I have considered and applied to render my opinions.

Claim Term	District Court Construction
“global perspective”	Not indefinite. Plain-and-ordinary meaning wherein the plain-and-ordinary meaning is “information about

Claim Term	District Court Construction
(cl. 1)1	events related to the monitored event across a network”
“wherein the global perspective for one or more related events to the at least one event across a network” (cl. 1)2	Not indefinite “wherein the global perspective [is] for one or more related events to the at least one event across [other devices on] a network”
“event line” (cl. 1)3	Plain-and-ordinary meaning
“gathering an event ... generating contextual state information for the event ... obtaining a global perspective for the event . . .” (cls. 1, 8, 16) 4	Order of steps: no order.

¹ EX-2008 8.

² EX-2008 9.

³ EX-2008 9.

⁴ EX-2008 10.

C. Level of Ordinary Skill In The Art

41. I understand that certain issues relating to the validity of the '045 patent must be judged from the perspective of a person of ordinary skill in the relevant art, as I discuss below. I have been asked to define the level of a “person having ordinary skill in the art” or “PHOSITA” that someone would have had at the time the alleged invention as claimed was made. In deciding the level of ordinary skill, I have considered the following factors, which I have been informed are relevant in determining the level of ordinary skill in the art:

- The levels of education and experience of persons working in the field;
- The types of problems encountered in the art;
- The prior art solutions to these problems;
- The rapidity with which innovations are made; and
- The sophistication of the technology.

42. In my opinion, a PHOSITA at the time of the invention of the '045 patent (around May 3, 2013) would have had a bachelor's degree in an accredited program of electrical engineering, computer engineering, or computer science or in a similar discipline, and have 2-3 years of practical work experience in the general fields of electrical engineering, networking, communications, and/or device and network security. More advanced degrees and/or training in a related discipline can compensate for shorter work experience.

43. I understand that Petitioner has defined the level of ordinary skill in the art as:

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.

(Petition, 7.)

44. Despite minor variations in these two positions, these variations would not alter my opinions expressed in this Declaration.

45. Based on either standard, I was at least a person of ordinary skill in the art at the time of the invention of the '045 patent.

V. PETITIONER'S GROUND 1 DOES NOT DISCLOSE OR RENDER OBVIOUS THE CHALLENGED CLAIMS

46. I understand Petitioner's first ground challenging the claims of the '045 Patent is as follows:

Ground 1	Section 103(a)	Obvious over Morris; alternatively, obvious over Morris in view of Van Oorschot	Claims 1-2, 4, 8-10, 12, and 16;
-----------------	----------------	---	----------------------------------

			alternatively, Claims 1-4, 8-10, 12, and 16
--	--	--	---

47. I understand that Petitioner and its expert allege that Morris or the combination of Morris and Van Oorschot renders obvious every limitation of the independent claims 1, 8, and 16, and that this allegation underlies their challenge of the remaining dependent claims 2-4, 9, 10, and 12. I disagree with the arguments in the Petition and opinions set forth by Dr. Lee for at least the reasons that I discuss in further detail in this section.

A. Overview Of Morris

48. Morris is titled “Methods and Apparatus for Dealing with Malware” and was filed on June 30, 2006 and published on January 18, 2007. (EX-1005.) Morris claims a system and method for classifying a computer object as malware. (EX-1005 [0001], cl. 1.) For example, claim 1 of Morris reads:

1. A method of classifying a computer object as malware, the method comprising:

at a base computer, receiving data about a computer object from each of plural remote computers on which the object or similar objects are stored;
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.
(EX-1005, cl. 1.)

B. Independent Claims 1, 8, And 16

1. Morris Does Not Disclose Or Render Obvious Limitations [1(b)], [8(e)(ii)], and [16(g)(i)]

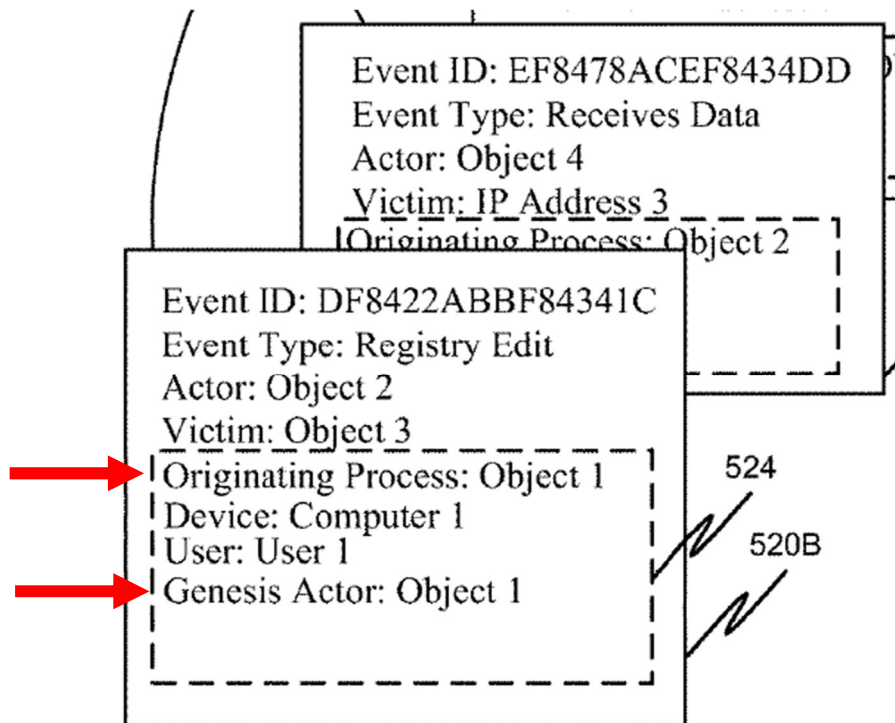
49. Petitioner relies on the same analysis of Morris to support Limitations 1(b), 8(e)(ii), and 16(g)(i) in Ground 1. (Petition 14-15, 32, 35-36.) These limitations recite the following language:

Limitation	Claim Language
1(b)	<i>“generating a contextual state for at least one of the one or more events by correlating the at least one event to an originating object”</i>
8(e)(ii)	<i>“generate a contextual state for at least one of the one or more events by correlating the at least one event to an originating object, the contextual state including an indication of the originating object of the first object”</i>
16(g)(i)	<i>“the contextual state including an indication of the originating object of the first object and an indication of at least one of a device on which the first object is executed and a user associated with the first object</i>

50. Petitioner contends that “Morris’s disclosure of correlating ‘GenesisActor’ data with an event is consistent with the ’045 Patent’s generating contextual state information.” (Petition 15.) But the Petition fails to acknowledge that the ’045 Patent explicitly distinguishes the GenesisActor from the “*originating object*.” (EX-1001 8:42-51.)

51. The ’045 Patent describes contextual state information as including originating processes or objects, devices, and users. (EX-1001 8:42-45, 17:30-35.) (Note that the ’045 Patent uses “originating process” and “originating object” interchangeably. *E.g.*, EX-1001 17:39-42.) Additionally, contextual state information may also include GenesisActor information, *i.e.*, the object that is “the ultimate parent of the event being performed.” (EX-1001 8:43-48.) That is, the ’045 Patent distinguishes between the originating process/object and the GenesisActor information.

52. This distinction is illustrated in Figure 5B. (EX-1001 Fig. 5B.) Figure 5B depicts context 520B as comprising an “originating process or object” separate and distinct from GenesisActor. (*Id.* 17:30-43.)



(EX-1001, Fig. 5B (excerpted and annotated).) “[A]s illustrated in Fig. 5B, the originating process or object may [be] determined based on a previous event that initiated or otherwise created the current process and/or object. Additionally, as illustrated in Fig. 5B, the GenesisActor is determined based on a chain of previous events.” (*Id.* 17:39-43.) The ’045 Patent further explains that “[a]lthough illustrated as including an originating process, GenesisActor, device, and user, the contextual information forming the contextual state 520B may include more or less information and in varying combinations.” (EX-1001 17:35-38.)

53. Claims 1 and 8 recite contextual state information that is generated “*by correlating the at least one event to an originating object*” and Claim 17 recites

contextual state information that “*including an indication of the originating object of the first object.*”

54. Petitioner’s repeated assertions that, because Morris discloses GenesisActor, Morris necessarily discloses contextual state information fails to satisfy the specificity of these limitations—*i.e.*, that contextual state information is generated “*by correlating the event to **an originating object of the first object***” or that the contextual state information includes “*an indication **of an originating object of the first object.***” Accordingly, Morris fails to teach these limitations.

55. My opinion is further supported by a PHOSITA’s understanding of these terms within the context of the ’045 Patent’s specification. Because the GenesisActor and the *originating object* identify distinct pieces of information, the distinction between each in malware detections could prove critical—for example, where the ultimate parent of an object (*i.e.*, the GenesisActor) does not provide contextual state information indicating a threat but information based on the *originating object* does indicate a threat. In such a circumstance, contextual state information generated based on the GenesisActor cannot serve as a proxy or provide the same benefit as contextual state information generated based on the originating object of the event.

56. Morris’s disclosure does not render obvious the challenged claim limitations, **nor does Petitioner argue that it does.** (Petition 14-15 (making no

assertion that Morris renders obvious this limitation).) Morris discloses various types of meta data that might be captured and evaluated through its heuristic processes. (EX-1005 [0104]-[0109].) For examples, Morris identifies meta data including: events—the actions or behaviors of an object acting upon another object; identities—the attributes of an object; GenesisActor—the ultimate parent of the event; ancillary data; and event checksums. (*Id.*) That is, Morris does not disclose capturing the originating object as part of the collected metadata. Thus, there is no suggestion or teaching by Morris, nor does Petitioner identify a single reason that a PHOSITA would have been motivated to modify Morris’s method to generate contextual state information by correlating the event to an originating object.

57. I note that Petitioner relies on a combination of Morris and Van Oorschot in its challenge of this limitation of Claim 1. However, the petition relies on Van Oorschot’s teachings only with respect to limitation 1(b)(i)’s unique portion of this limitation—“*an indication of at least one of a device on which the first object is executed [or] a user associated with the first object.*” Therefore, Petitioner’s combination of Morris and Van Oorschot still relies on Morris’s teachings as allegedly disclosing limitation 1(b)’s “*generating contextual state information for the event by correlating the event to an originating object of the first object,*” which it does not do. Accordingly, the petition does not show a prior art teaching of these limitations under Ground 1.

2. The USPTO’s Allowance of the ’224 Continuation Patent Further Supports My Opinion

58. I understand that Morris shares a common inventor with U.S. Patent Application Publication No. 2012/0260340 (“Morris 340”), which incorporates Morris (the prior art at issue in this proceeding) and which was before the Examiner during prosecution of the U.S. Patent No. 10,257,224 (“the ’224 continuation patent”). (EX-2022 p.2 (citing Morris 340 as prior art).) The ’224 continuation patent is a continuation of the ’045 patent and contains highly-similar claims and the same specification. (*Compare* EX-1001 with EX-2022.)

59. I understand that during prosecution of the ’224 continuation patent, the International Searching Authority provided a written opinion analyzing Morris 340 in detail, considering the same arguments Petitioner now presents in its Petition. (*Compare* EX-1002 270 (considering whether “Gensesisactor” information is “*originating object*” information) *with* Petition 14–15 (same)); *compare* EX-1002 270 *with* Petition 16–17 (same considerations regarding “*obtaining a global perspective*” limitation). Thus, the USPTO’s previous allowance of the ’224 continuation patent over Morris 340 further supports my opinion—discussed in detail above—that Morris’s highly similar disclosures do not disclose or render obvious the challenged claims.

C. Dependent Claims

60. Because neither Morris nor the combination of Morris and Van Oorschot render obvious all limitations of the independent claims, I understand that Ground 1 also fails to render obvious dependent claims 2-4, 9, 10, and 12 as well.

VI. PETITIONER’S GROUND 2 DOES NOT DISCLOSE OR RENDER OBVIOUS THE CHALLENGED CLAIMS

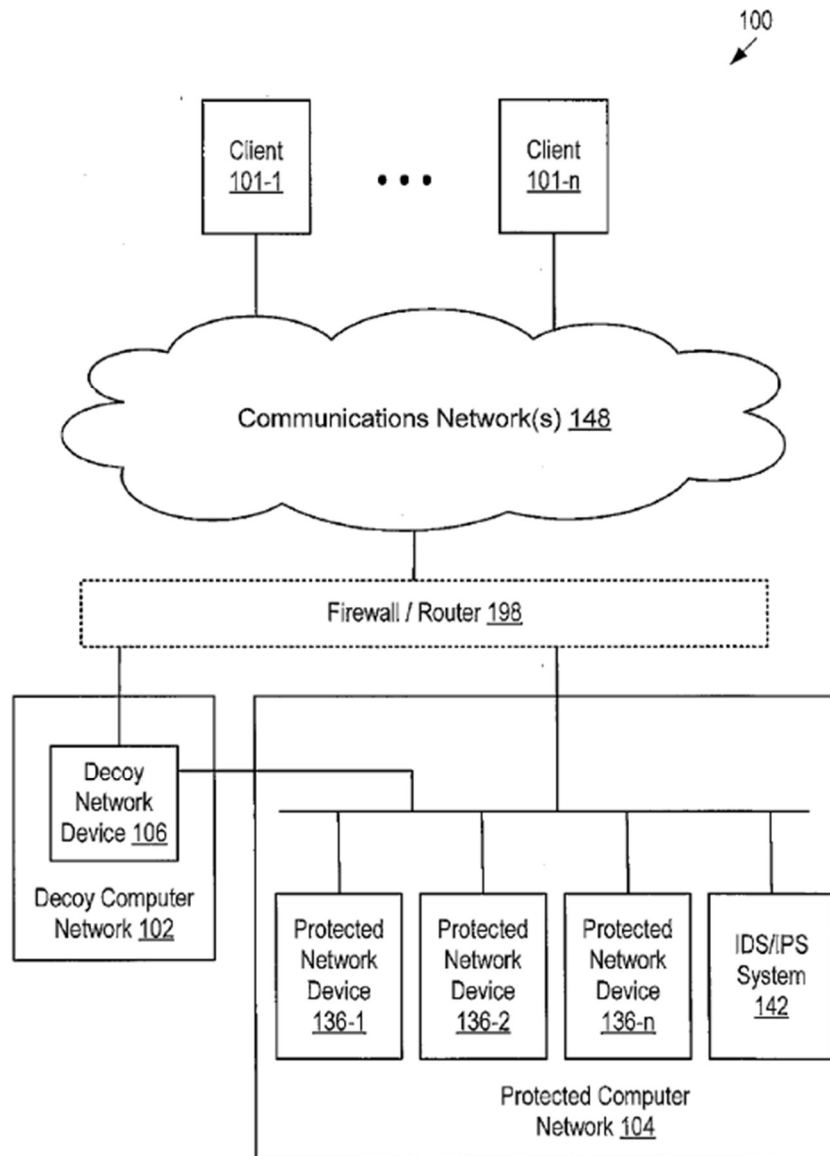
61. I understand Petitioner asserts an additional ground challenging the claims of the ’045 Patent:

Ground 2	Section 103(a)	Obvious over Capalik in view of Van Oorschot	Claims 1-4, 7-8, 10-13, 16-19
-----------------	----------------	--	-------------------------------

A. Overview Of Capalik

62. Capalik sought to fulfill the purported “need for efficient methods of identifying fingerprint data for previously unknown types of malicious and/or unauthorized activities,” recognizing that many network security systems relied on malware fingerprints to identify potentially malicious attacks. (EX-1008 [0007]-[0008].) Thus, Capalik is directed to a system and method for generating a profile, or “fingerprint,” for a computer object after supervising its activities on a virtual machine. (EX-1008 Abstract; cl. 1.)

63. Capalik discloses a system and method implemented via a decoy network device—*i.e.*, a decoy system that is monitored to collect fingerprint data of unauthorized activities. (EX-1008 [0030], Fig. 1.)



(EX-1008 Fig. 1.) “The purpose of the decoy network device 106 is 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. This fingerprint of the attack can be used to prevent similar attacks on the decoy network device 106 and/or other computers (e.g., protected network devices 136.” (EX-1008 [0030].) The decoy network device utilizes a virtual machine—*i.e.*, one or more software applications

emulating one or more physical machines—to establish virtual or decoy operating systems to attract attacker activity. (EX-1008 [0052]-[0053].)

64. Capalik teaches a method for monitoring activities on this virtual machine. (EX-1008 [0010].) Because a decoy system’s virtual machine “typically does not actively send and receive packet streams over the network (because the purpose of the decoy system is to wait for a potential attack from an attacker),” “any incoming packet stream 304 of data is treated as an unauthorized activity.” (*Id.* [0068], Figs. 3A-3D, 4A-4E.) Activities are identified using their source, target, and the association between the source and target, and recorded. (EX-1008 [0010].)

65. A fingerprint indicative of the activity on the virtual machine is created from the stored activities and is transmitted to identify the attack on other affected systems. (EX-1008 [0010]; *see also* Figs. 6A–C (flowchart).) Thus, unlike malware identification and mitigation solutions that generation information from monitoring a computer object’s activity on devices across a network, Capalik is directed to generating information about a computer object’s activities on a single decoy device. “The decoy network device creates (636) the fingerprint indicative of the activity on the virtual machine from the stored activities.” (EX-1008 at [0120].)

66. Capalik’s decoy network device architecture is illustrated in Fig 2, which shows the host operating system on a decoy device memory running the virtual machines, which are running decoy operating systems:

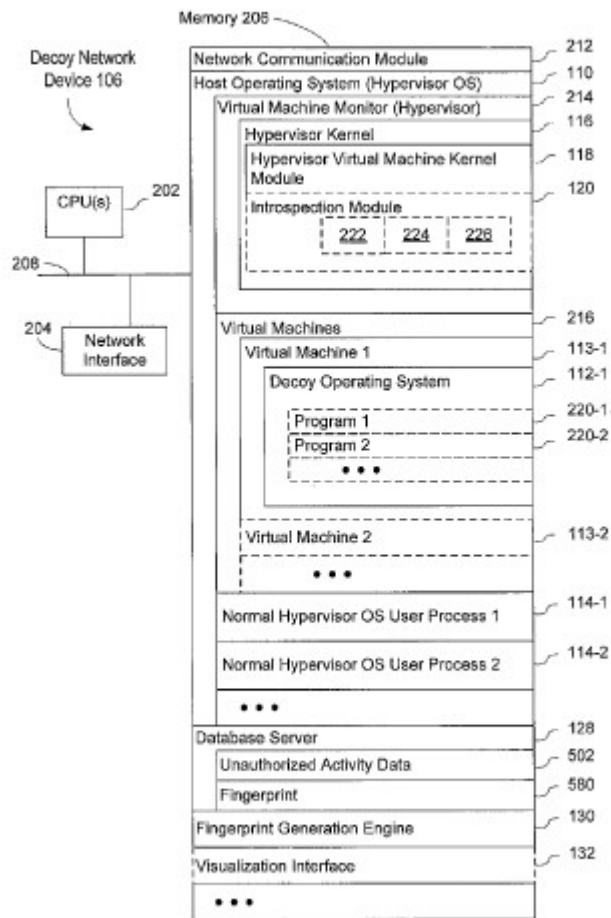


Figure 2

(EX-1008 Fig. 2, [0052]-[0054].)

67. Referencing Claim 1, Capalik claims:

1. A computer implemented method of identifying unauthorized activities on a decoy computer system attached to a computer network, wherein the decoy system comprises:
 - one or more processors; and
 - memory storing;
 - a virtual machine; and
 - a virtual machine monitor supervising the virtual machine, the method comprising at the virtual machine monitor:
 - monitoring activity on the virtual machine;

identifying a plurality of activities being performed at the virtual machine, wherein each of the activities includes an activity source, an activity target, and an association between the activity target;

storing in the memory the activity sources, activity targets, and associations;

creating, from the stored activities, a fingerprint indicative of the activity on the virtual machine; and

transmitting the fingerprint to prevent future attacks that comprise the same or similar activities as indicated by the fingerprint.

(EX-1008 cl. 1)

B. Independent Claims 1, 8, And 16

1. Capalik Does Not Disclose Or Render Obvious Limitations [1(c)(ii)], [10(e)(v)], And [17(e)(iii)]

68. Claims 1, 8 and 16 of the '045 patent include the limitation “wherein the global perspective for one or more related events to the at least one event across a network.” Petitioner relies on the same analysis of Capalik to support Limitations [1(c)(ii)], [8(e)(iii)], and [16(h)] in Ground 2. (Petition, 50-52, 63, 67.) These limitations recite the following language:

Limitation	Claim Language
[1(c)(ii)], [8(e)(iii)]	<i>“wherein the global perspective for one or more related events to the at least one event across a network”</i>

[16(h)]	<i>“global perspective information comprising information about one or more related events to the one or more events across a network”</i>
---------	--

69. Petitioner and its expert’s argument relies on a single quote and figure from Capalik’s specification—but these disclosures do not support Petitioner’s argument.

70. First, Petitioner asserts that Capalik discloses global perspective information that relates to one or more events across a network, because Capalik teaches 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.” (Petition 50.) But Petitioner’s conclusion does not follow from this teaching and is, in fact, contradicted by Capalik’s structure.

71. As discussed in detail above, Capalik teaches that is invention may be implemented through the use of a decoy network device. (*See* Section VI(A), *supra*.) Capalik explains that a decoy computer device may include one or more virtual machines, each of which may include a decoy operating system. (EX-1008 [0052]-[0053].) A “virtual machine monitor” supervises the virtual machine. (*Id.* [0011].) Capalik teaches that the virtual machine monitor includes a “hypervisor kernel,” which may provide basic services to the virtual machine monitor. (*Id.* [0045].) The hypervisor kernel supports virtualization of the decoy operating system and

“includes an introspection module 120” which monitors “the physical memory segments assigned to each of the virtualized decoy operating system 112.” (*Id.* [0046].) That is, a single decoy device’s introspection module monitors memory segments associated with one or more decoy operating systems ***on the same device***. (*See id.*) Because all of the virtualized operating systems are on the same device, following a chain of unauthorized activity across multiple virtualized operating systems still does not disclose “*one or more other events related to the event across a network*.” Thus, Capalik’s teaching still does not disclose a “*global perspective*” that “*relates to one or more other events related to the event across a network*.”

72. Second, Petitioner contends that Figure 4E depicts a scenario in which global perspective information is obtained “based on related events from multiple data streams across a network”:

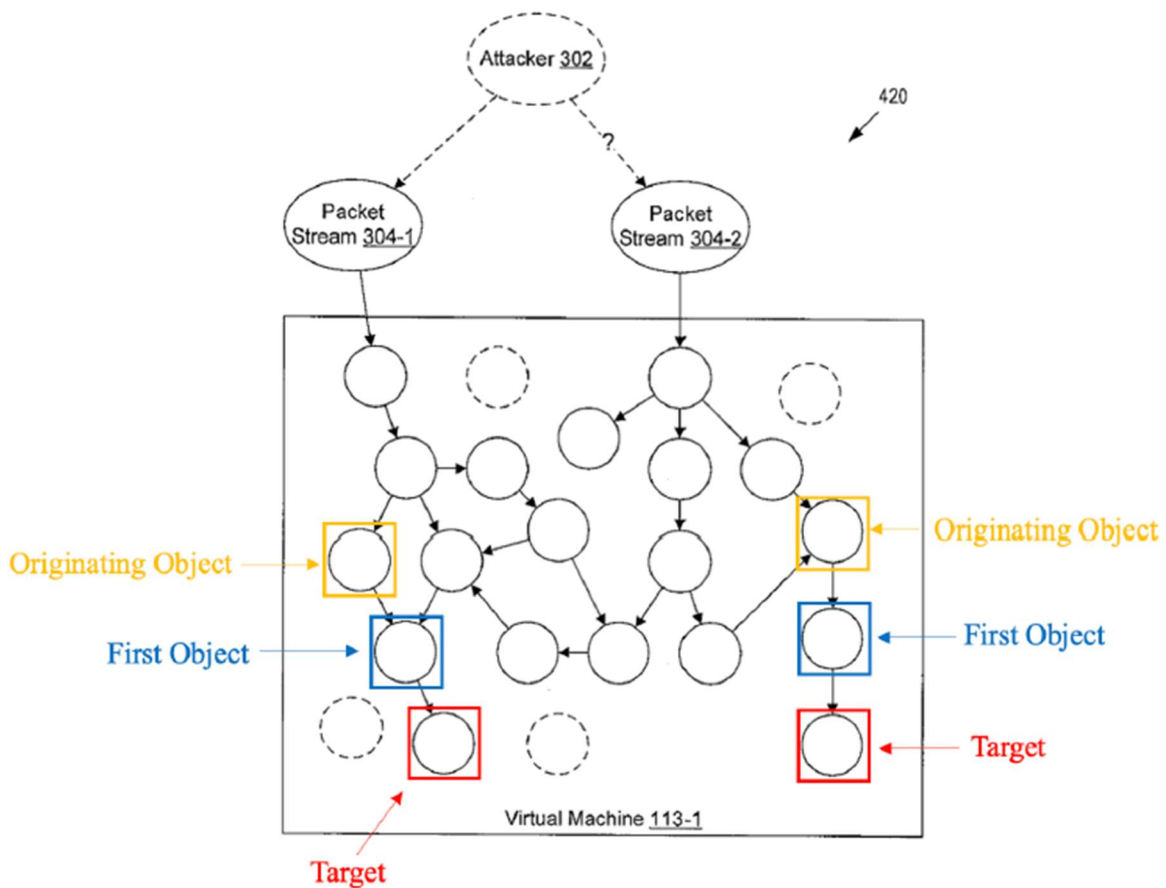


Figure 4E

(Petition 52.)

73. But again, Figure 4E illustrates unauthorized activities on “*the virtual machine 113-1*”—*i.e.*, a single virtual machine on a single decoy device. (EX-1008 [0074].) Capalik teaches that because virtual machines do not typically send and receive data packets over a network, “any incoming packet stream 304 of data is treated as an unauthorized activity.” (*Id.* [0068], Fig. 4E.) In Figure 4E above, “multiple packets of data streams (e.g., 304-1 and 304-2) are detected, and all activity on the computer system 498 are monitored and recorded.” (*Id.* [0074].)

74. Capalik’s recording of events and associations on a single decoy device—even if across multiple virtualized operating systems—does not disclose a “*global perspective*” that “*relates to one or more other events related to the event across a network.*”

75. Petitioner does not argue that a PHOSITA would have been motivated to modify Capalik’s teachings, nor would a PHOSITA be motivated to do so. Even if one were to utilize multiple decoy network devices, Capalik does not disclose how such a system would operate. For example, Capalik does not instruct a PHOSITA on how the generated fingerprint is used by other devices on a network or how one would modify computer systems on a network to use the fingerprint—only that it can be used. (EX-1008 [0127] (“[i]n some embodiments, one or more other computer systems (e.g., protected network devices 136) on the network are modified (646) to prevent future attacks that comprise the same or similar activities as indicated by the fingerprint (e.g., in FIG. 1A, the IDS/IPS system modifies at least one of the protected network devices(s) 136 to prevent future attacks that comprise the same or similar activities.”).) Additionally, Capalik does not teach that the devices would necessarily share information and/or analysis in the process of generating malware fingerprints. And Capalik does not explain whether resulting fingerprints would be mutually shared or merely stored on the single decoy device that generated them. Capalik only discloses a single decoy network device’s monitoring of activity

restricted to the same device. (*E.g.*, EX-1008 Fig. 4E.) Accordingly, Capalik does not disclose or render obvious these limitations.

76. I note that Petitioner relies on a combination of Capalik and Van Oorschot in its challenge of Claim 3 under Ground 2. However, the Petition does not rely on Van Oorschot's teachings with respect to the limitations of any independent claim. (*See generally* Petition 37-69.)

2. The USPTO's Allowance Of The '224 Continuation Patent Further Supports My Opinion

77. I understand that Capalik shares a common inventor with U.S. Patent Application Publication No. 2008/0016570 ("Capalik 570" or Exhibit 1030), which includes the same "decoy computer network" architectures, *i.e.*, a series of virtual machines running on a single device, and which was considered during examination of the '224 continuation patent at the USPTO as a secondary reference. (EX-1002 292-294.)

78. Furthermore, I understand that during prosecution of the '224 continuation patent, the Examiner initially rejected independent claim 1 in view of U.S. Patent Application Publication No. 2013/0298244 ("Kumar" or Exhibit 1004)—in particular, Kumar's disclosure of obtaining a global perspective to a specific device. (EX-1002 293.) In overcoming this rejection, the Applicant argued:

It is illogical to conclude that such a simplistic mapping of alerts to a specific device is analogous to the claimed "global perspective" that is

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

(EX-1002 293 (emphasis added).) Capalik’s disclosure on which the Petition relies is the substantively the same as Kumar’s disclosure—over which the Examiner ultimately allowed the ’224 continuation patent. Accordingly, the allowance of the ’224 Patent over Kumar further supports my opinion—discussed in detail above—that Capalik’s highly similar disclosures do not disclose or render obvious the challenged claims.

C. Dependent Claims

79. Because neither Capalik nor the combination of Capalik and Van Oorschot render obvious all limitations of the independent claims, I understand that Ground 2 fails to render obvious dependent claims 2-4, 7, 9-10, 12, 15, 17, and 18 as well.

VII. CLAIMS AND/OR LIMITATIONS NOT ADDRESSED IN THIS DECLARATION

80. It is my understanding that this declaration is being provided in support of Patent Owner’s Preliminary Response. Because the prior art is so clearly deficient,

I have provided analysis of key limitations not included in the prior art. My decision not to analyze particular limitations or claims in no way indicates or supports that these limitations or claims are disclosed or rendered obvious by the prior art, and I reserve the right to supplement my analysis if asked to do so.

VIII. SECONDARY OBJECTIVE INDICIA OF NONOBVIOUSNESS

81. I understand that in determining obviousness of the claimed invention, objective evidence of secondary considerations pertaining to nonobviousness must be considered, including long-felt but unsolved needs, failure of others, commercial success, etc. (*In re Huang*, 100 F.3d 135, 139 (Fed. Cir. 1996) (citing *Graham*, 383 U.S. at 17-18).) I further understand that these indicia constitute independent evidence of nonobviousness that can be the most probative evidence in that regard “in avoiding the trap of hindsight when reviewing, what otherwise seems like, a combination of known elements.” (*Leo Pharm. Prods., Ltd. v. Rea*, 726 F.3d 1346, 1358 (Fed. Cir. 2013).)

82. As demonstrated by my summary of the prior art, above, there was a long-felt and persistent need to improve network forensics methods prior to the invention of the '045 Patent. (*See* Section III, *supra*.) Prior attempts to develop reliable network security were limited in their ability to establish any sort of context or obtain useful information from within the host or system, making them insufficient to identify and address the threats faced by modern computer networks. (*See* Section

III, *supra.*) Where others failed, the '045 Patent succeeded. (*See* Section IV(A), *supra.*)

83. Thus, these secondary indicia only further support my opinion that the '045 Patent was non-obvious.

IX. CONCLUSION

84. For the foregoing reasons, it is my opinion that Petitioner's grounds do not render obvious any of the challenged claims of the '045 Patent.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Executed this 20th day of March, 2023 in Los Angeles.

Respectfully submitted,

A handwritten signature in blue ink, appearing to read 'N Medvidovic', with a long horizontal flourish extending to the right.

Nenad Medvidovic, Ph.D.