

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

AO KASPERSKY LAB,
Petitioner,

v.

OPEN TEXT INC.,
Patent Owner.

IPR2023-00124
Patent 9,578,045 B2

**PETITIONER'S REPLY TO
PATENT OWNER'S RESPONSE**

LIST OF EXHIBITS

Exhibit Number	Exhibit Name
1001	US Patent No. 9,578,045 to Jaroch et al.
1002	File History of U.S. Patent No. 9,578,045
1003	Declaration of Dr. Wenke Lee
1004	U.S. Publication No. 2013/0298244 to Kumar et al.
1005	U.S. Publication No. 2007/0016953 to Morris et al. (“ <i>Morris</i> ”)
1006	U.S. Patent No. 8,087,087 to Van Oorschot et al. (“ <i>Van Oorschot</i> ”)
1007	U.S. Publication No. 2010/0077481 to Polyakov et al (“ <i>Polyakov</i> ”)
1008	U.S. Publication No. 2011/0321166 to Capalik et al. (“ <i>Capalik</i> ”)
1009	U.S. Publication No. 2012/0260340 to Morris et al. (“ <i>Morris</i> ”)
1010	U.S. Patent No. 10,257,224
1011	Scheduling Order (Dkt. 50)
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)
1013	SANS Institute, <i>Host- vs. Network-Based Intrusion Detection Systems</i> (2000-2005)
1014	Securosis LLC, <i>Evolving Endpoint Malware Detection: Dealing with Advanced and Targeted Attacks</i> , Version 1.3 (July 12, 2012)
1015	Yanfeng 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)
1016	U.S. Patent No. 6,944,772 to Dozortsev
1017	U.S. Patent No. 6,772,346 to Chess et al.
1018	WO 2002/033525 to Shyne-Song Chuang
1019	EP 1,549,012 to Kristof De Spiegeleer
1020	EP 1,280,040 to Alexander James Hinchliffe et al.
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)
1022	U.S. Patent Publication No. 2004/0143753 to Hernacki et al.
1023	U.S. Patent Publication No. 2011/0083180 to Mashevsky et al.
1024	U.S. Patent No. 8,429,746 to Alen Capalik

1025	Server Hardware, Software and Architecture by <i>Abeer El Hadi El Zein El Nahas, University of Khartoum, Electrical and Electronics Engineering Dept. (Feb. 2008)</i>
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 16 th USENIX Security Symposium (August 2007)
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 27 th Annual Computer Security Applications Conference (December 2011)
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)
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)
1030	<i>Plaintiffs' Markman Opposition Brief</i> (Dkt. 98)
1031	<i>Defendants' Markman Opening Brief</i> (Dkt. 86)
1032	EPO File History for Application No. 14791882.5
1033	Declaration of Hunter Horton in Support of Motion for Pro Hac Vice
1034	Confidential Agreement
1035	Webroot, Inc. and Open Text Inc., v. AO Kaspersky Lab. et al., Case No. 6:22-cv-243-ADA-DTG, Joint Claim Construction Statement, Dkt. 185 (W.D. Tex. Feb. 20, 2023)
1036	Robert Sedgewick, Algorithms in C: Graph Algorithms (3rd ed.), Pearson Education, (2002)
1037	David B. Guralnik, Webster's New World Dictionary of the American Language, (1984)

TABLE OF CONTENTS

LIST OF EXHIBITS.....	i
TABLE OF CONTENTS	iii
I. INTRODUCTION	1
II. THE CLAIMS DO NOT REQUIRE THE ORIGINATING OBJECT TO BE THE OBJECT THAT DIRECTLY INITIATED OR OTHERWISE CREATED THE FIRST OBJECT	1
A. Patent Owner’s construction of “originating object” is improper	1
B. Ground 1 renders obvious generating contextual state for at least one of the one or more events by correlating the at least one event to an originating object.....	4
III. THE CLAIMS DO NOT REQUIRE THE END RECIPIENT DEVICE TO BE A DEVICE THAT IS SEPARATE FROM THE DEVICE AND THAT INCLUDES THE SENSOR AGENT AND THE GLOBAL PERSPECTIVE INFORMATION SERVER.....	6
A. Patent Owner’s construction of “end recipient device” is improper	6
B. Ground 1 renders obvious 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.....	8
IV. GROUND 1 RENDERS OBVIOUS A “SENSOR AGENT”	9
A. <i>Morris</i> discloses a sensor agent operable to generate contextual state information for at least one of the one or more events by correlating the at least one event to an originating object	9
B. <i>Morris</i> discloses a sensor agent operable to gather an event defining an action of a first object acting on a target	11
V. GROUND 2 RENDERS OBVIOUS A GLOBAL PERSPECTIVE THAT RELATES TO ONE OR MORE OTHER EVENTS RELATED TO THE EVENT ACROSS A NETWORK.....	14
VI. VAN OORSCHOT RENDERS OBVIOUS AN EVENT PRIORITY BASED ON THE GENERATED CONTEXTUAL STATE IN GROUND 1 AND GROUND 2	18

VII. CONCLUSION 19

CERTIFICATION UNDER 37 CFR § 42.24(d).....21

CERTIFICATE OF SERVICE 22

I. INTRODUCTION

Patent Owner's Patent Owner Response (POR) relies on improper claim constructions and flawed reasoning in an attempt to elide the actual disclosures of the references. Indeed, PO rewrites the claims to change "originating object" as the "the object that directly initiated or otherwise created the first object" and "end recipient device" as "a device that is separate from the device that includes the sensor agent and the global perspective information server." Neither change is warranted.

For these reasons, the Board should follow the evidence and find the Challenged Claims unpatentable.¹

II. THE CLAIMS DO NOT REQUIRE THE ORIGINATING OBJECT TO BE THE OBJECT THAT DIRECTLY INITIATED OR OTHERWISE CREATED THE FIRST OBJECT

A. Patent Owner's construction of "originating object" is improper

Patent Owner asks the Board to interpret the "originating object" as "the object that directly initiated or otherwise created the first object." POR, 18. Conversely, in the associated litigation, Patent Owner resisted construction of the term, arguing for

¹ Petitioner files this Reply consistent with the November 29, 2023, email communication from the Board in which the Panel indicated it would extend Due Date 2 (Petitioner's Reply) to December 28, 2023, and Due Date 3 (Patent Owner's Surreply) to February 8, 2024.

no construction other than an unidentified “plain and ordinary meaning.”² Adding such language to the language of claim 1 is improper and represents an impermissible attempt to amend the claim language without the proper procedure of a motion to amend. *See SuperGuide Corp. v. DirecTV Enters., Inc.*, 358 F.3d 870, 875 (Fed. Cir. 2004)(“[A] particular embodiment appearing in the written description may not be read into a claim when the claim language is broader than the embodiment.”). Any motion to amend must comply with the content requirements of 37 C.F.R. §§ 42.121(b) or 42.221(b).

Additionally, Patent Owner has not satisfied the stringent requirements associated with a disclaimer of claim scope. “To disavow claim scope, the specification must contain ‘expressions of manifest exclusion or restriction, representing a clear disavowal of claim scope.’” *Retractable Techs., Inc. v. Becton, Dickinson & Co.*, 653 F.3d 1296, 1306 (Fed. Cir. 2011) (quoting *Epistar Corp. v. Int’l Trade Comm’n*, 566 F.3d 1321, 1335 (Fed. Cir. 2009)). Here, the ‘045 Patent’s specification does the opposite, making clear “the [first] object, the event, and the target are then correlated to **at least one originating object**” (i.e., potentially more than one)—not a single object that must also be **the object that directly initiated/created** the first object. ‘045 patent, Abstract, emphasis added. The specification further refers

² Ex. 1035, p. 7. Consistent with Patent Owner’s request, the Court did not construe the term. Ex. 2024, p. 10.

several times to “originating processes” and correlating to “one or more originating processes,” further demonstrating that a singular directly initiating originating object was not intended. ‘045 patent at 8:42-43; 12:57-59; 12:63-66; 20:63-65. There is no further definition in the specification of the ‘045 patent further limiting the scope of “originating object.”

Patent Owner asserts, citing the ‘045 specification, “[t]he originating object refers to “a previous event that initiated or otherwise created the current process and/or object.”” POR, 14. The excerpt cited by Patent Owner actually reads “[m]oreover, as 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.” The permissive “may” is used and, as such, there is no basis to narrow the claim scope. Moreover, this sentence makes clear that the originating object is merely “a previous event” and not necessarily “the immediately preceding event,” which is further evidenced by the use of plurals and “at least one” in reference to originating processes, as discussed above. Further, this sentence makes clear that the originating object “initiated” the current object. That is, an initiation does not mean an originating object has to be “**the** object that **directly** initiated” the first object.

Based on these disclosures, a POSITA would have understood the ultimate parent of an object to be an example of an originating object within the meaning of the ‘045 Patent. “[A]bsent ‘clear and unmistakable’ language suggesting otherwise, we conclude that the aforementioned statements do not meet the ‘exacting’ standard

required to limit the scope of the claims.” *Cont'l Circuits LLC v. Intel Corp.*, 915 F.3d 788, 798 (Fed. Cir. 2019) (citation omitted).

This and Patent Owner’s other attempts to improperly limit the scope of the Challenged Claims are unsupported by the law and should be rejected.

B. Ground 1 renders obvious 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

As set forth in the Petition, a “GenesisActor” is the ultimate parent object of the event being performed. More particularly, among all the objects in the sequence that lead to the event correlated with the first object, which are all originating objects, the GenesisActor is the very first/starting one in the sequence and is, therefore, an originating object. Petition, 16; *Morris*, [0058], [0107]. A GenesisActor is an originating object because it is an object from a previous event that initiated the chain of events that lead to the current event involving the current process and/or object (“first object”).³

³ Patent Owner asserts that the “originating object refers to ‘a previous event that initiated or otherwise created the current process and/or object.’” POR, 14, citing the ‘045 patent at 17:40-42. However, Patent Owner’s selective citation misstates the actual language of the ‘045 patent, which actually reads, “the originating process or object may be determined based on a previous event that initiated or otherwise created the current process and/or object” thereby conflating the terms “object” and “event.”

Citing its expert, Patent Owner asserts that “the GenesisActor may provide less helpful contextual state information than the originating object.” POR, 14. The quality (*e.g.*, “less helpful”) of contextual state information provided by the GenesisActor is irrelevant. The GenesisActor provides such information, which is all that the claim requires. As discussed above, however, a GenesisActor is an originating object just like other objects in the sequence of events leading to a current event of the first object. Moreover, since a GenesisActor is an originating object and the very first in the sequence, it not only provides contextual state information at the beginning of the chain of actions but also facilitates the identification of all the subsequent originating objects in the sequence (including the one that immediately precedes the first object) and their contextual state information. Petition, 17; *Morris*, [0099], [0105].

Citing its expert, Patent Owner further asserts that “skipping to the ultimate parent” would result in an incomplete event audit trail due to gaps between the immediate parent and the ultimate parent because the ’045 patent uses the claimed “originating object” to create a full audit trail “to forensically track back any event which occurs to what triggered it.” POR, 17. However, no “skipping” is involved. A POSITA would have understood that going “forward” from a GenesisActor originating object as the starting point and the first object as the end point using well-known graph traversal algorithms such as depth-first search is just as feasible as “tracking back” to

‘045 Patent, 17:39-42.

obtain all the subsequent objects in the sequence leading to the first object to create the full audit trail. The direction of traversal is the same algorithmically and provides a full audit trail. See Ex. 1036, pp. 94, 101 (discussing depth-first search, “[t]o visit a vertex, we mark it as having been visited, then (recursively) visit all the vertices that are adjacent to it and that have not yet been marked... The critical fact remains that DFS visits all the edges and all the vertices connected to the start vertex, *regardless of in what order* it examines the edges incident on each vertex,” emphasis in original). Moreover, the disclosure in the ‘045 Patent to “forensically track back” is with reference to an administrator end recipient interacting with the audit trail *after* the audit trail has been created, not with reference to how the audit trail is created. ‘045 Patent, 12:60-13:2. The claim does not recite generating contextual state information by forensically tracking back.

Therefore, *Morris* renders obvious generating contextual state information for the event by correlating the event to an originating object of the first object.

III. THE CLAIMS DO NOT REQUIRE THE END RECIPIENT DEVICE TO BE A DEVICE THAT IS SEPARATE FROM THE DEVICE AND THAT INCLUDES THE SENSOR AGENT AND THE GLOBAL PERSPECTIVE INFORMATION SERVER

A. Patent Owner’s construction of “end recipient device” is improper

Patent Owner asks the Board to interpret “end recipient device” to be “a device that is separate from the device that includes the sensor agent and the global perspective information server.” POR, 21. But there is no disclosure in the

specification or language in the claim to justify Patent Owner's interpretation. Adding such language to the language of claim 10 is improper and represents an impermissible attempt to amend the claim language without the proper procedure of a motion to amend. *SuperGuide*, 358 F.3d 875; 37 C.F.R. §§ 42.121(b), 42.221(b).

Moreover, in the associated litigation, Patent Owner did not ask for the term "end recipient device" to be construed, and the term was not construed. POR, p. 10-12; see Ex. 2024, p. 10. Patent Owner has now provided a convoluted proposed construction. In particular, it is unclear whether Patent Owner intends the "end recipient device" to be separate from *one* component ("the device that includes the sensor agent and the global perspective information server") or if Patent Owner intends the "end recipient device" to be separate from *two* components ("the device that includes the sensor agent" *and also* separate from "the global perspective information server").

Regardless, Patent Owner has now asked for a construction that is in conflict with the district's court's construction and in conflict with the fact that Patent Owner failed to ask for such a construction during claim construction at the district court. Patent Owner's new attempts to improperly limit the scope of the Challenged Claims should be rejected.

B. Ground 1 renders obvious 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 explained in the Petition, *Morris* discloses base computer 3 and database 7 as a group of devices receiving and analyzing data, providing global perspectives, and generating new signatures. *Morris*, [0014]-[0017], [0020], [0078]; Petition, 32-35. *Morris* accordingly discloses that the computer 3 and database 7 operate with remote computer 2, consistent with the '045 specification. Petition, 34; IPR2023-00124 Ex. 1003, ¶¶150-153.

Patent Owner asserts that the base computer 3 of *Morris* cannot be the claimed end recipient device because *Morris* purportedly does not “disclose[] or render[] obvious a remote computer transmitting an event line to another remote computer.” POR, 56. However, that is not what claim 10 recites. Rather, the claim requires that the “sensor agent transmits the event line to the end recipient device.” *Morris* discloses that 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. *Morris*, [0020]; IPR2023-00124 Ex. 1003, ¶153.

As explained in the Petition and by Dr. Lee, in *Morris*, remote computer 2, has a sensor agent that sends event line data to base computer 3, an end recipient device. To be clear, neither the Petition nor Dr. Lee assert that the remote computer 2 is using its sensor agent to send the same event line to itself. The event line (key) sent from

base computer 3 to remote computer 2 is for new or updated malware information, not the exact same information that remote computer 2 already has, e.g., in its local database. IPR2023-00124 Ex. 1003, ¶¶153, 117 (“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).

Therefore, *Morris* renders obvious the claimed end recipient device.

IV. GROUND 1 RENDERS OBVIOUS A “SENSOR AGENT”

A. *Morris* discloses a sensor agent operable to 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

Patent Owner asserts that the Petition fails to show how *Morris* discloses a sensor agent operable to generate contextual state information of claim 8. POR, 45-48. However, as explained in the Petition and Dr. Lee’s declaration, *Morris*’ sensor agent (local agent software on a remote computer 2) “generate[s] contextual state information for the event by correlating the event to an originating object of the first object.” Petition, 32; IPR2023-00124 Ex. 1003, ¶¶142-148, 82-85.

In *Morris*, the data sent to the base computer 3, that is, the data collected by the sensor agent on a remote computer 2, includes:

at least three severable components, a first of said components representing executable instructions contained within or constituted by the object, a second of said components representing data about said

object, and a third of said components representing the physical size of the object. The data about the object in the second component may be any or all of the other forms of identity such as the file's name, its physical and folder location on disk, its original file name, its creation and modification dates, vendor, product and version and any other information stored within the object, its file header or header held by the remote computer 2 about it; and, events initiated by or involving the object when the object is created, configured or runs on the respective remote computers. In general, the information provided in the key may include at least one of these elements or any two or more of these elements in any combination.

Morris, [0087], *see also* [0018]. In particular, paragraph [0087] of *Morris* makes clear that the “events initiated by or involving the object when the object is created, configured or runs” provide “contextual state information for the event including an originating object of the first object,” as claimed.

Dr. Lee’s deposition testimony further explained this point.

Q. ... So is the event that is being gathered in the claims of the '224 patent on the remote computer in *Morris*?

A. I would say that, here, the event really -- you know, so here the language “events initiated by or involving the object when the object is created, configured or runs on the respective remote computers.” That really meets the limitation of the claim saying gathering an event, defining an action of a first object acting on a target. So that's what I'm trying to say.

Ex. 2025, 188:17-189:6 (quoting *Morris* [0087]); *see also* Ex. 2025, 189:12-190:1.

The fact that the base computer will do more analysis based on data sent from a plurality of remote computers does not negate the fact that each remote computer generates contextual state information for the event by correlating the event to an originating object of the first object and then sends such data (i.e., key) to the base computer for further analysis.

Therefore, *Morris* renders obvious the claimed sensor agent operable to generate contextual state information.

B. *Morris* discloses a sensor agent operable to gather an event defining an action of a first object acting on a target

Patent Owner asserts that the Petition fails to show how *Morris* discloses a sensor agent operable to gather an event of claims 8 and 16. POR, 45-48. However, as explained in the Petition and Dr. Lee's declaration, the events gathered at the remote computer 2 by the sensor agent already include information about a global perspective. Referring to paragraph [0018] as cited in the Petition, "vendor, product and version" indicate where the file came from (e.g., where on the Internet this file came from) and roughly when it was updated (e.g., when this version was released), etc." *Morris*, [0018]; Petition, 12-14; IPR2023-00124 Ex. 1003, ¶¶77-81.

Dr. Lee's deposition testimony further explained that remote computer 2 searches the local database about an event first. The local database has the up-to-date global perspective information previously sent from database 7/base computer 3 (e.g., an event line in the form of a new/updated key). In other words, whatever relevant event information the global perspective information server (database 7/base computer

3) already has, the remote computer has it too. Therefore, the remote computer 2 has up-to-date global perspective information of the event.

A. So, again, the paragraph I'm referring to that this refers to really is in the context of the Claim 12, global perspective communication server. And that's paragraph 112 talking about that one, meaning that what the global perspective information server in this case, base computer 3, in conjunction with database 7, what would they do. But if you read the *Morris* patent, Figure 2 talks about what the remote computer could do, to get the same perspective, is search the local database.

Q. Well, earlier today you testified that the global perspective is something that's not local. That's, in fact, global and not local. Right? So

—

A. Hold on, hold on, hold on. You misquoted me. I was saying that the global perspective would be only considering information has no external input. Okay? And if you read further of the *Morris* spec, it talks about how the local database get[s] updated by the global perspective information server. So basically your local server has the information from the global perspective server, so we have external input. So if you use that information to draw a conclusion, that's global perspective. It's not local.

Ex. 2025, 198:7-199:9.

Plainly, *Morris* discloses that base computer 3 performs further analysis, e.g., correlating data sent from multiple remote computers, to generate the updated or new event information. However, this does not negate the fact that the remote computer also has such information and/or gets new/updated information from the global

information server.

Patent Owner further asserts that the Petition asserts that the base computer in *Morris* “gathers” events initiated by or involving the object when the object is created, configured or runs on the respective remote computers, with reference to paragraph [0018]. POR, 45-48. Patent Owner is wrong. The Petition makes clear that remote computer 2 gathers the event. Citing to paragraph [0078] of *Morris*, the Petition explains, “[r]emote 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.” Further, citing to paragraph [0081] of *Morris*, the Petition explains, 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.” Citing to paragraphs [0078] and [0086] of *Morris*, the Petition further explains that this information is passed in “the form of a so-called signature or key relating to the object and its effects.” Petition at 11, emphasis added. And, paragraph [0018] of *Morris* actually discloses, “the data about the computer object that is sent from the plural remote computers to the base computer and that is used in the comparison includes... events initiated by or involving the object when the object is created, configured or runs on the respective remote computers.” *Morris*, [0018]. Thus, *Morris* makes quite clear that a remote computer sends such data to the base computer and hence the remote computer (e.g., by local agent software) must have gathered such data in the first place.

Therefore, *Morris* renders obvious the claimed sensor agent operable to gather an event defining an action of a first object acting on a target.

V. GROUND 2 RENDERS OBVIOUS A GLOBAL PERSPECTIVE THAT RELATES TO ONE OR MORE OTHER EVENTS RELATED TO THE EVENT ACROSS A NETWORK

With reference to the claimed global perspective, Patent Owner asserts that in *Capalik*, all of the virtualized operating systems are on the same device, “so there is no ‘one or more other events related to the event across a network.’” POR, 60. In selectively quoting and truncating the claim language, Patent Owner implies that the limitation requires that the global perspective *use* or *incorporate* events from other devices on a network. Not so.

The language omitted by Patent Owner’s selective quotation is instructive. Claim 1 actually recites, “wherein the global perspective for one or more related events *relates to* the at least one event across a network,” emphasis added. Thus, the natural reading of the limitation is that the global perspective need only have some connection with (related to) another event, the other event being experienced by another device on a network and having some connection with (related to) the event experienced on the local device. *Capalik* provides such connections. See Ex. 1037 (definition of “related” as “connected or associated”).

Capalik makes quite clear that its decoy network device 106 is one of multiple devices within decoy computer network 102. *Capalik*, [0030]. Because of the text accompanying Figure 1, a POSITA would understand that each decoy network device

within the decoy computer network may be a separate device and would be connected to the rest of the decoy network devices by a network, similar to the protected network devices within the protected computer network. Further, a POSITA would understand that each decoy network device would be connected (through a network) to the protected computer network and also each protected network device because the connection is shown in Figure 1. *Capalik* further teaches that a POSITA would understand that the methods with respect to monitoring the decoy network device “may be used for monitoring one or more non-decoy systems, such as the protected network devices 136.” *Capalik*, [0032]. Therefore, while Figure 2 in *Capalik* may be described as being a single machine, a POSITA would understand that Figure 2 and the Figure 2 description would apply to all decoy network devices within the decoy computer network and would apply to all non-decoy systems on which monitoring has been implemented (not just a single device as Patent Owner contends), all of which are connected by a network.

Capalik further describes “[t]he decoy computer network 102 **includes one or more decoy network device(s) 106,**” and that the entire “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.” (Emphasis added.) Accordingly, “decoy network device 106 is intentionally kept vulnerable to unauthorized or malicious activities (e.g., known security weaknesses may be intentionally left unfixed or other security components (e.g., firewalls) are

intentionally not installed).” *Capalik*, [0030].

Accordingly, the entire purpose of *Capalik* is to draw connections between attacks on decoy network device 106 and other devices. In fact, “[t]he decoy network device 106 includes security devices and software applications **like other protected network devices** (e.g., the decoy network device 106 may be protected by the firewall/router 198 and any other security measures included in the protected network devices 136).” *Capalik*, [0030], emphasis added. Such security devices and software applications “like other protected network devices” is an example of the disclosed relatedness or connection between events across networked devices because an event (e.g., unauthorized activity) would operate on decoy network device 106 like the other protected network devices.

The Petition explains *Capalik’s* activity source 512 and activity target 514 are evidence of the claimed *action of a first object acting on a target*. Petition, 41-42. In further explaining activity source 512 and activity target 514, *Capalik* discloses:

the analysis engine is configured to maintain several layers of network diagrams. . . . For example, a low-level layer might consist of a process reading from a file and subsequently writing many new files. In some cases, the analysis engine might identify this low level pattern as a representation of a file archive being unpacked, and generate a higher-level layer that includes an unpacking process. This exemplary generalization **allows the system to identify common elements of attacks**, identify classes of attack that have not been seen before (e.g., zero-day attacks), and generate higher-quality signatures.

Capalik, [0129], emphasis added. *Capalik* therefore describes maintaining layers of network diagrams in order to identify related events or connections (e.g., common elements of attacks) between networked devices.

As explained in the Petition, *Capalik*'s analysis is "able to follow a **chain of unauthorized activity** across multiple virtualized operating systems." *Capalik*, [0130], emphasis added. Patent Owner argues that "Petitioner does not explain why activity across virtualized **operating systems** on a single device would be understood by POSITA as equivalent to activity across a **network**." POR, 65 (emphasis in original).

However, this argument misses the point. First, *Capalik* discloses use of "one or more decoy network device(s) 106," not just a single device as Patent Owner contends. *Capalik*, [0030]. Notably, these multiple decoy network devices 106 reside on a network ("Decoy Computer Network 102"). *Capalik*, Fig. 1. As such the chain of unauthorized activity is in fact evidence of activity data (an event) with a connection to commonalities in the activity between decoy network device 106 and other networked devices. As taught by *Capalik*, "[t]his is important in identifying and thwarting advanced threats that involve multiple attackers spread **across multiple systems**." *Capalik*, [0130], emphasis added.

Accordingly, *Capalik* discloses a global perspective that "relates to one or more other events related to the event across a network," as claimed. Patent Owner's truncation of the claim language distorts the limitation and is erroneous. Accordingly,

Petitioner's use of *Capalik* to make its obviousness case is supported and invalidates the '045 patent.

VI. VAN OORSCHOT RENDERS OBVIOUS AN EVENT PRIORITY BASED ON THE GENERATED CONTEXTUAL STATE IN GROUND 1 AND GROUND 2

Patent Owner asserts that *Van Oorschot's* "severity level" cannot be the claimed event priority because it is not based on generated contextual state information that includes an indication of the originating object. POR, pp. 56-57. This assertion is incorrect because the attributes disclosed in Van Oorschot provide information about "the originating object." *Van Oorschot*, 7:12-27; *see also* Petition, 57-58; IPR2023-00124 Ex. 1003, ¶¶200-204, 63-67. These disclosed attributes include a contextual state of an event, including the actor, i.e., "who", which can be a user or a software tool, etc., the "action", i.e., "what", and the object/victim of the action, i.e., "on what." *Id.* As one example, when a user or software tool creates a file, then the user or software tool is an "originating object" of the event (create) and the first object (file). *Id.*

As explained in the Petition and by Dr. Lee, Van Oorschot's assignment of severity levels inform a recipient of the relevance of the event. Petition, 57-58; IPR2023-00124 Ex. 1003, ¶¶200-204, 63-67. *Van Oorschot* discloses that its severity level is assigned based on the context related to the event. The attributes of an event are used to decide the security level according to "significance factor(s)" assigned to the attribute groups. *Van Oorschot*, 7:27-32. Such attributes include:

the “when” attribute may include groups that define time elements, such as “office hours”, “weekends”, or “weekdays”. The “who” attribute may include groups related to the various forms of users, such as “network administrators” or “general users”. The “what” attribute may include groups related to the types of actions that can occur, such as “file write actions”, “file read actions”, “administrative actions”, or “email transfer”. The “on what” attribute may include, for example, groups related to the types of files being operated on. The “where”, “where from”, and “where to” attributes may include groups related to the types of clients at which the event can occur, the types of clients initiating the event, or the types of clients being acted upon by the event, for example “web servers”, “test servers”, “mail servers”, “file servers”, “workstations”, or “database servers”.

Van Oorschot, 7:12-27.

These attributes disclosed in *Van Oorschot* provide information about “the originating object.” *Van Oorschot*, 7:12-27; *see also* Petition, 57-58; IPR2023-00124 Ex. 1003, ¶¶200-204, 63-67.

Accordingly, *Van Oorschot* renders obvious an event priority based on generated contextual state information that includes an indication of the originating object.

VII. CONCLUSION

For these reasons, the Board should find the challenged claims of the ‘045 Patent to be unpatentable.

Respectfully submitted,

Dated: December 28, 2023

/s/ Joseph T. Miotke

Joseph T. Miotke, Reg. No. 47,798

Eric H. Chadwick, Reg. No. 41,664

Erin Block, Reg. No. 78,154

DeWitt LLP

901 Marquette Avenue

Suite 2100

Minneapolis, MN 55042

T: (612) 305-1400

F: (612) 305-1414

jtm@dewittllp.com;

ehc@dewittllp.com;

eblock@dewittllp.com;

docketing@dewittllp.com

Attorneys for Petitioner

CERTIFICATION UNDER 37 CFR § 42.24(d)

Under the provisions of 37 CFR § 42.24(d), the undersigned hereby certifies that the word count for the foregoing Petitioner Reply to Patent Owner Response to Petition totals 4,776, which is allowed under 37 CFR § 42.24(c)(1).

Respectfully submitted,

Date: December 28, 2023

/s/ Joseph T. Miotke

Joseph T. Miotke, Reg. No. 47,798
Eric H. Chadwick, Reg. No. 41,664
Erin Block, Reg. No. 78,154
DeWitt LLP
901 Marquette Avenue
Suite 2100
Minneapolis, MN 55042
T: (612) 305-1400
F: (612) 305-1414
jtm@dewittllp.com;
ehc@dewittllp.com;
eblock@dewittllp.com;
docketing@dewittllp.com

CERTIFICATE OF SERVICE

Pursuant to 37 CFR § 42.6(e)(4), the undersigned certifies that on December 28, 2023, a complete and entire copy of this Petitioner Reply to Patent Owner Response and supporting exhibits were provided via email, to the Patent Owner by serving the email correspondence address of record as follows:

Brian Eutermoser, Reg. No. 64,058
Russell E. Blythe, Reg. No. 58,440
Mikaela Stone, Reg. No. 70,404

KING & SPALDING LLP
1401 Lawrence Street,
Suite 1900
Denver, CO 80202

Email: beutermoser@kslaw.com
Email: rblythe@kslaw.com
Email: Mikaela.stone@kslaw.com

/s/ Rachel Gagliardi
Rachel Gagliardi
DeWitt LLP
901 Marquette Avenue
Suite 2100
Minneapolis, MN 55042