

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

TREND MICRO, INC.

Petitioner

v.

OPEN TEXT INC.

Patent Owner

Case IPR2023-00657

Patent No. 10,257,224

**DECLARATION OF PROFESSOR NENAD MEDVIDOVIC, Ph.D.
IN SUPPORT OF PATENT OWNER'S PRELIMINARY RESPONSE**

TABLE OF CONTENTS

II.	QUALIFICATIONS	2
III.	UNDERSTANDING OF RELEVANT LEGAL PRINCIPLES	7
IV.	STATE OF THE PRIOR ART	10
V.	THE '224 PATENT	11
	A. Summary of the '224 Patent.....	11
	B. Claim Construction	14
	C. Level Of Ordinary Skill In The Art.....	16
VI.	OVERVIEW OF PRIOR ART	18
	A. Overview of Rockwood (EX-1004)	18
	B. Overview of Xie (EX-1005).....	24
	1. Anomaly Detection Using Spatiotemporal Correlation.....	24
	2. Network forensics using spatiotemporal event correlation	26
VII.	ROCKWOOD IN VIEW OF XIE DOES NOT DISCLOSE OR RENDER OBVIOUS THE CHALLENGED CLAIMS.....	27
	A. Rockwood's Does Not Gather Information about Objects Acting on Targets or Executing on Devices	29
	1. The "Network Layer/OS" Is Not a "First Object"	30
	2. Rockwood Does Not Disclose or Render Obvious an Event Defining a First Object Acting on a Target	33
	B. The Rockwood-Xie Combination Does not Disclose or Render Obvious the "Originating Object"	36
	C. POSITA Would Not Have Been Motivated to Combine Rockwood with Xie Because Each Reference Embodies the Problems of the Prior Art	42

D.	Rockwood Does Not Obtain a Global Perspective for the Event	44
E.	Rockwood in View of Xie does Not Disclose or Render Obvious an Event Line Comprising Information Relating to the Event	46
F.	Dependent Claims	50
VIII.	CLAIMS AND/OR LIMITATIONS NOT ADDRESSED IN THIS DECLARATION	50
IX.	SECONDARY OBJECTIVE INDICIA OF NONOBVIOUSNESS	51
X.	CONCLUSION.....	52

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., 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)
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. and Open Text Inc., v. AO Kaspersky Lab. Et al.</i> , Case No. 6:22-cv-243-ADA-DTG, Dec. 9, 2022 Transcript of Motions Hearing, Dkt. 133 (W.D. Tex. Dec. 15, 2022) (excerpted)
2008	Dani Kass, “Catching Up On Patent Litigation With Judge Albright” (Law360 Mar. 14, 2023); https://www.law360.com/pulse/articles/1582438/print?section=pulse/courts
2009	U.S. District Courts – Federal Court Management Statistics – Profiles – During the 12-month Periods Ending March 31, 2018 Through 2023, “Table N/A – U.S. District Courts – Combined Civil and Criminal Federal Court Management Statistics (March

Exhibit	Description
	31, 2023)”, available https://www.uscourts.gov/sites/default/files/data_tables/fcms_na_distprofile0331.2023.pdf
2010	<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)
2011	<i>Webroot, Inc. and Open Text Inc., v. Trend Micro Inc.</i> , Case No. 6:22-cv-00239-ADA-DTG, Defendant Trend Micro’s Preliminary Invalidity Contentions (W.D. Tex., Sept. 13, 2022)
2012	<i>Webroot, Inc. and Open Text Inc., v. Trend Micro Inc.</i> , Case No. 6:22-cv-00239-ADA-DTG, Plaintiff’s Preliminary Infringement Contentions (W.D. Tex., July 13, 2022)
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)
2014	<i>Webroot, Inc. and Open Text Inc., v. Trend Micro Inc.</i> , Case No. 6:22-cv-00239-ADA, Complaint for Patent Infringement, Dkt. 1 (W.D. Tex., Mar. 4, 2022)
2015	<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)
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)

Exhibit	Description
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	<i>Webroot, Inc. and Open Text Inc., v. CrowdStrike, inc. and CrowdStrike Holdings, Inc.</i> , Case No. 6:22-cv-002410ADA-DTG, Defendant's Preliminary Invalidity Contentions (W.D. Tex., Sept. 13, 2022)

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 10,257,224 (“the ’224 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 ’224 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 ’224 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 have reviewed and my knowledge and professional judgement. In forming the opinions expressed in this Declaration, I reviewed the Petition for *Inter Partes* Review of U.S. Patent No. 10,257,224 and supporting exhibits.

5. I have been asked to provide my technical opinions on how concepts in the '224 patent specification relate to claim limitations of the '224 patent. In reaching the opinions provided herein, I have considered the '224 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.

II. 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 nearly 30 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 10 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 16th ACM SIGSOFT International Symposium on the Foundations of Software Engineering and at the 44th International Conference on Software Engineering. I am currently serving

as General Co-Chair of the 21st International Conference on Software Architecture (ICSA 2024).

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 SIG-SOFT, 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.

III. 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 predicable 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 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:

27. I have been informed that a prior art reference may be relied upon not only for what it expressly teaches, but also for what is inherent therein—i.e., what necessarily flows from the express teachings. I further understand that the mere fact that a certain thing may result from a given set of circumstances is not sufficient.

IV. STATE OF THE PRIOR ART

28. Network forensics generally relates to intercepting and analyzing network events to discover the source of security attacks. (EX-1001 1:24-26.) At the time of the invention of the '224 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 1:26-35.) Such network forensics tools passively collect network traffic and reside at a network edge, e.g., a location where an organization's network interfaces with the internet. (See EX-1001 1:35-45.) Although network edge devices may receive network events, they cannot establish any sort of contextual information about the event from within the host or system generating the event. (See EX-1001 1:42-45.)

29. As a result, network forensics tools could not obtain useful information from within a host or establish any sort of context with information about the event from within a host that was generating and/or receiving network events. (*See* EX-1002 385-86.) Without this information, prior art network forensics tools were insufficient to identify and address threats faced by modern computer networks. (*See* EX-1001 1:48-51.)

30. Although a network edge device may be able to 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 2:7-14.) The network edge device thus had no way of knowing to what extent a virus may have impacted computing devices on the network, what additional files may have become infected, or what operating processes and/or objects are linked to the virus. (*See* EX-1001 2:14-18.)

31. Accordingly, there was a long-felt need for an improved forensic visibility technique to efficiently determine whether computer objects were malware.

V. THE '224 PATENT

A. Summary of the '224 Patent

32. The '224 patent is entitled “Method and Apparatus for Providing Forensic Visibility into Systems and Networks,” and describes and claims a system and

method that improved on traditional network forensics tools used to discover or identify security issues on computer networks.

33. Unlike traditional network forensics tools, the '224 patent creates forensic visibility *into* the computing devices on the communication network to identify malware or other security issues in the operation of those devices. (EX-1001 2:38-40.) In particular, the '224 patent improves network security by gathering an “event,” generating “contextual state information,” obtaining a “global perspective” for the event, generating an “event line” comprising information relating to the “event,” and transmitting the generated “event line” that includes information for the event. (*See* EX-1001 cl. 1.) The described and claimed systems and methods collect endpoint 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.

34. In addition to analyzing the behavior of objects to identify those that are potentially malicious, malware detection is further improved by understanding the context of the event and computer objects of interest. (EX-1001 2:41-45 (“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.’”).) As the applicant argued during prosecution:

[T]he claims are directed to a specific improvement in computer functionality relating to computer security, and more specifically to providing **end-to-end visibility of events** within a system and/or network The Specification subsequently discusses a variety of ways in which the claimed subject matter solves the above-described problem [O]ne aspect of the present disclosure to provide a system and method whereby **events occurring within a computing device are captured** and additional context and a global perspective is provided for each capture event.

(EX-1006 87-88.) (emphasis added) In many cases, a potentially malicious object is identified by the system as a result of other events that provide information relevant to whether the code is malicious.

35. The ’224 patent further explains that, in addition to contextual information, the patented systems and techniques can also use information from the network to obtain a global perspective of the network’s operation. 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.

36. The '224 patent further discloses technical improvements to forensics systems by “assembling” or “generating” an “event line” based on the contextual information and global perspective. (EX-1001 9:57–65.) 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 address any damage inflicted by an originating object. (EX-1001 9:52–56.)

37. Thus, the '224 patent describes and claims systems and methods that provide more efficient and accurate identification of malware and improve the identification of other malware (and corresponding events) that might otherwise go undetected in prior art systems, thereby improving system performance and reducing required resources.

B. Claim Construction

38. Petitioner states that no dispute exists over the construction of claim terms for the purposes of its petition. (Petition 10-11.) On March 16, 2023, the district court concluded that no terms of the '224 patent were indefinite and construed

all terms as having their plain and ordinary meaning.¹ (EX-2010 8-11.) In its claim construction order, the Court construed independent claims 1 to require generating contextual information before obtaining the global perspective, as set forth below:

Claims	Claim Term	Court's Construction
1, 10, 17	“gathering an event defining an action of a first object acting on a target, wherein the first object is executed on a device; generating contextual state information for the event by correlating the event to an originating object of the first object; obtaining a global perspective for the event based on the contextual state information, wherein the global perspective comprises information associated with one or more of the first object and the	’224 Patent, Claim 1: No order between [1A] and [1B], but the “contextual information” in [1B] must precede the obtaining of the “global perspective” in [1C].

¹ The court provided additional clarifying remarks regarding certain terms’ plain and ordinary meaning. For brevity and because all but one of those clarifications are not critical to the issues addressed in the preliminary response—other than the Court’s remarks regarding the requisite order of steps for claim 1, which I have provided above—I do not reproduce all those clarifying remarks here and instead cite the district court’s claim construction order as an exhibit.

Claims	Claim Term	Court's Construction
	originating object, and wherein the global perspective relates to one or more other events related to the event across a network;””	

Accordingly, I apply the plain and ordinary meaning of all claim terms, including the Court's stepwise ordering for claim 1.

C. Level Of Ordinary Skill In The Art

39. I understand that certain issues relating to the validity of the '224 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 “POSITA” that someone would have had at the time the 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.

40. A POSITA at the time of the invention of the '224 patent had a bachelor's degree in an accredited program of electrical engineering, computer engineering, or computer science, or a similar discipline, and have 2–3 years of practical work experience in the general fields of electrical engineering, computer science, networking, communications, and/or device and network security. More advanced degrees and/or training in a related discipline can compensate for shorter work experience.

41. I understand that Petitioner and its expert have defined the level of ordinary skill in the art as:

A person having ordinary skill in the art [] at the time of the earliest claimed priority date for the '224 patent would have had a bachelor's degree in computer science, or a related field, or an equivalent technical degree or equivalent work experience, and an additional one to two years of education or experience in the field of computer security topics such as malware/exploit detection and/or network forensics. More education can supplement practical experience and vice versa.

(Petition 10.)

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

43. Based on either standard, I was at least a person of ordinary skill in the art at the time of the invention of the '224 patent.

VI. OVERVIEW OF PRIOR ART

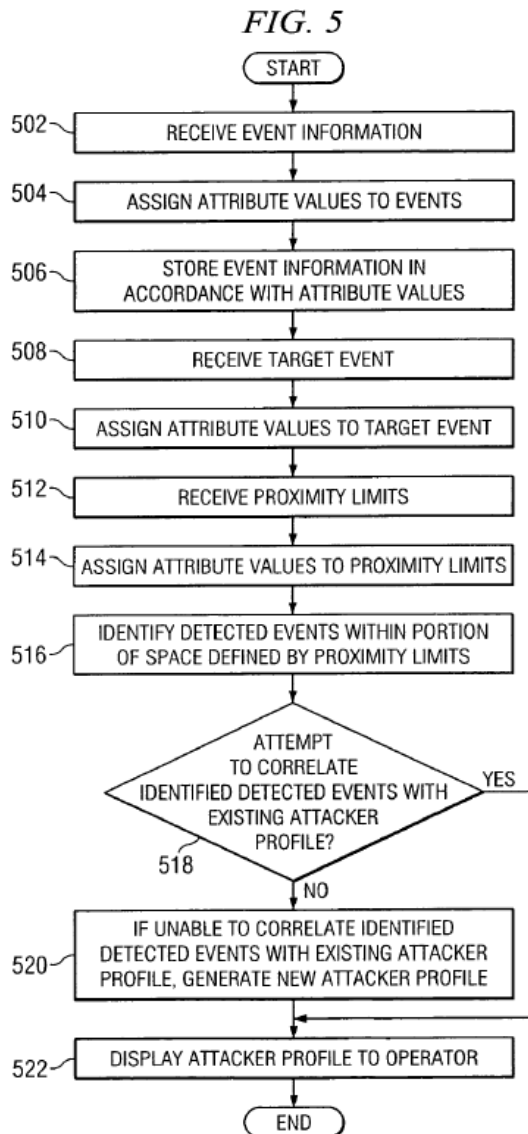
A. Overview of Rockwood (EX-1004)

44. Rockwood performs data collection with a hardware configuration that uses sensors located at a network port that receives TCP/IP packets or other similar communications from network 100. *See, e.g.*, EX-1004 2:40-45; 3:36–41; 14:52-57, Fig 1; Fig. 6. Rockwood's configuration matches the prior art system discussed in the '224 patent, where sensors (i.e., network sniffers) are located at network edges, monitoring traffic without the capability to link into network endpoints. *Compare* EX-1004 3:36-49 ("Each sensor 20 is located at a network port that receives TCP/IP packets or other similar network communications from network 100. These packets and similar network communications received by sensors 20 are referred to as detected events 110.") *with* EX-1001 1:36-51 ("However, existing network forensic tools, such as network sniffers and packet capturing tools, passively collect information about network traffic. Such tools may be able to detect and capture information associated with communication sessions, such as hostnames, ports, protocols, IP addresses, etc.; however, such tools tend to receive network events outside of a host or system. . . . Accordingly, network edge devices *have no ability to*

establish any sort of context from within the host or system that is generating the event.”) (emphasis added).

45. Rockwood’s sensors are network edge devices that collect information transmitted through a network port. (EX-1004 3:36-49.) Unlike the ’224 patent’s collection agents, Rockwood’s sensors do not collect information from within the endpoints, such as the contextual state information, regarding an observed event because they reside at the network edge. Thus, Rockwood’s event processing does not include contextual state information such as the originating event of an observed event and does not create an event line.

46. Rockwood processes events in isolation and does not trace the chain of events within an endpoint. Rockwood’s event information processing is illustrated by Figure 5:



(EX-1004 Fig. 5)

47. Rockwood abstracts each event into a point in n-dimensional space for subsequent analysis and forensic malware visualization. (EX-1004 Abstract, 1:40–56, Fig. 10). The point is translated to an n-dimensional vector with n elements,

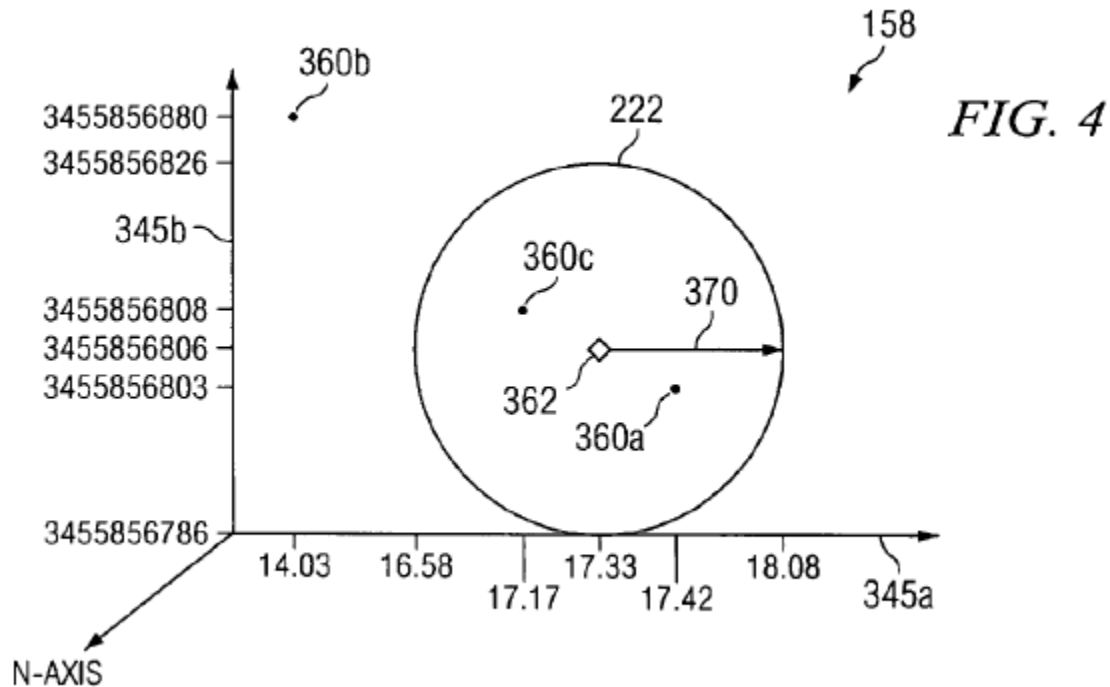
where each element is an attribute of the event (e.g., time, IP address). (EX-1004 1:40-46, Figs. 3, 4.)

FIG. 3

	410a	410b	410c	420a	420b	420c	
	ATTRIBUTE	ATTRIBUTE	ATTRIBUTE	ATTRIBUTE VALUE	ATTRIBUTE VALUE	ATTRIBUTE VALUE	
110a	DETECTED EVENT	5:25 P.M.	205.252.48.163	192.187.23.220	17.42	3455856803	3233486812
110b	DETECTED EVENT	2:02 P.M.	205.252.48.240	192.187.23.206	14.03	3455856880	3233486798
110c	DETECTED EVENT	5:10 P.M.	205.252.48.168	192.187.23.102	17.17	3455856808	3233486694
364	TARGET EVENT	5:20 P.M.	205.252.48.166	192.187.23.110	17.33	3455856806	3233486702
370	PROXIMITY LIMITS	45 MINUTES	20	30	0.75	20	30

EX-1004, Fig. 3.

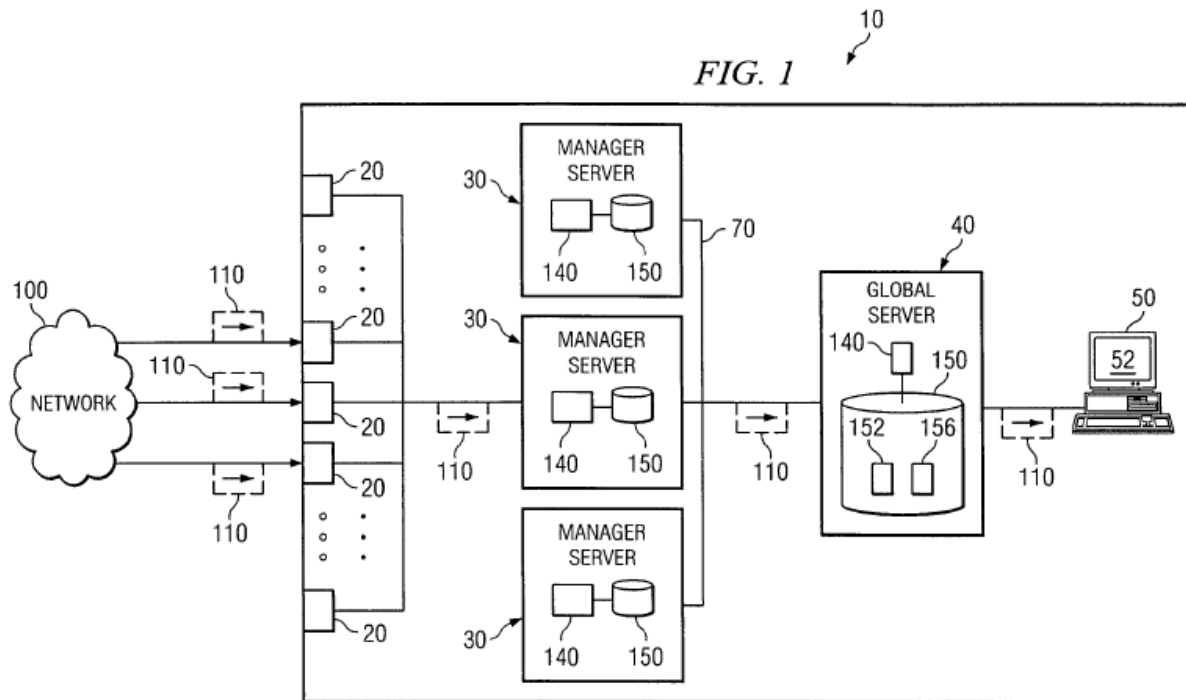
48. With these generated n-dimensional points, an incoming event can be compared against known malicious events based on the distance between the points that represent the incoming event and the malicious events. (*See, e.g.*, EX-1004 1:46-46; 9:31-46, Fig. 4.)



EX-1004 Fig. 4.

49. Rockwood’s “console” does not process event information. Rather, the console merely provides a user-friendly graphical user interface to display tailored and filtered information about detected events. (EX-1004 5:27-59 (“Intrusion detection system 10 may communicate the event information of detected events 110 to console 50 so that a user, such as an operator, may view and process the event information of detected events 110. . . . Console 50 may include a graphical user interface (GUI) 52 that tailor and filters the data presented to the user. Generally, GUI 52 provides the operator of console 50 with an efficient and user-friendly presentation of event information of detected events 110.”).) Rockwood’s event processing is

instead performed by backend servers (manager server 30 or global server 40), as illustrated by the intrusion detection system Fig. 1:



50. Rockwood’s intrusion detection system “comprises a plurality of sensors 20, one or more manager servers 30, global server 40, and console 50.” (EX-1004 2:40-48 (“Intrusion detection system 10 performs data collection using sensors 20. The data is correlated by manager servers 30 and/or global server 40.”). The manager server “represents any hardware or software module that controls or monitors one or more servant nodes, such as sensor 20. . . . [E]ach manager server 30 includes a correlation engine 140 and a ruleset 152 for receiving and correlating detected events 110 from sensors 20. Generally, through correlating and aggregating

detected events 110, manager server 30 is capable of detecting an attack or potential attack spread among sensors 20.” (EX-1004 4:5-17.) The global server “represents any hardware, software, firmware, or combination thereof operable to process, control, and monitor system 10 at the highest logical level” and, “[a]ccording to certain embodiments, global server 40 comprises a correlation engine 140. Correlation engine 140 is operable to correlate detected events 110 to detect an attack occurring upon or within the enterprise.” (EX-1004 4:39-67.)

B. Overview of Xie (EX-1005)

51. Xie is a Ph.D thesis titled “A Spatiotemporal Event Correlation Approach to Computer Security.” (EX-1005 1.). Xie addresses two separate applications of spatiotemporal event correlation: anomaly detection and network forensics. (EX-1005 1.) Anomaly detection is based on abnormal file changes *within a given computer*, and using those file changes to identify patterns of file updates that are shared across multiple hosts. (EX-1005 1.) In contrast, network forensics focuses on identifying the *source node* and *attack flows* (instead of source object) of detected malware based on statistical processing of network traffic. (EX-1005 1.)

1. Anomaly Detection Using Spatiotemporal Correlation

52. In Xie’s anomaly detection technique, the state change of a given computer (referred to in Xie as “state transition”) is abstracted into an n-dimensional

point or n-dimensional vector. (EX-1005 1, 25-26, 29-30.) Each element in this n-dimensional vector represents whether a selected file changes. (EX-1005 1, 25-26, 29.) In other words, the anomaly detection technique selects n files to monitor; and if any of them changes (for any reason, whether legitimate or due to malware), the element in the n-dimensional vector representing this file acquires a specified value (e.g., 0 or 1). (*See, e.g.*, EX-1005 25-26, 30, 33-34.)

53. Anomaly detection is then performed by monitoring the clustering of these n-dimensional points. For legitimate file changes, the n-dimensional points tend to cluster around a known location. (EX-1005 30.) In contrast, file changes caused by malware tend to create abnormal clusters. (*See, e.g.*, Figure 2.1 at EX1005-31.). This is illustrated in Xie by Figure 2.1, below:

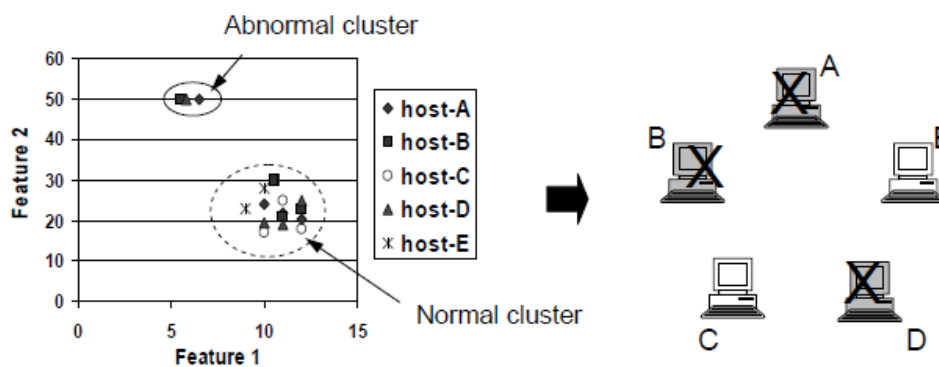


Figure 2.1: Pointillist approach to anomaly detection. Normal points are clustered by the dashed circle. The appearance of a new cluster consisting of three points suggests anomalous events on host A, B, and D.

54. Xie's anomaly detection does not identify the originating file/object or process of any instance of detected malware and does not assemble an event line.

2. Network forensics using spatiotemporal event correlation

55. Xie's network forensics technique aims to identify the true source, i.e., the original computer, of an internet attack, especially when "indirection" (e.g., using "stepping stones" or "zombies") is involved. (EX-1005 59.) Many types of internet attacks use indirection as a means to hide their source. (EX-1005 59.) For example, using a chain of compromised machines, or "stepping stones," a common means of foiling a defender's attempts to locate the source of an attack. (EX-1005 59-60.) Similarly, distributed denial-of-service (DDoS) attacks are often launched from compromised computers, sometimes called "zombies," both to harness the power of many machines and to obfuscate where the true source of the attack lies. (EX-1005 59-60.)

56. Xie's identification process includes collecting network traffic *between computers* that are being monitored and performing Monte Carlo sampling (e.g., random walk algorithm) to reveal the "initial attack path" that leads to the true source computer. (See, e.g., EX1005 59-60 67, 128.)

57. Xie's network forensics technique generates a *causal tree* between *different computers* in a network. (See, e.g., EX-1005 63, 62-63, Figs 3.3 (where each oval represents a host node).) This is unlike the '224 patent, which looks at different computer objects within a given computer—not different host nodes, i.e., computers.

58. To collect all network traffic among different nodes, Xie teaches the use of sensors or “auditing devices” for the intrusion detection system’s traffic logging. (EX-1005 64-66; *see also* 78, Figure 3.12 (where the traffic is collected from the *backbone* of a university network).) In this aspect, the architecture of network forensics in Xie is similar to that of Rockwood, and they suffer similar deficiencies, including the inability to look inside endpoints to collect contextual information around an observed event.

VII. ROCKWOOD IN VIEW OF XIE DOES NOT DISCLOSE OR RENDER OBVIOUS THE CHALLENGED CLAIMS

59. Petitioner and its expert allege that Rockwood in view of Xie renders obvious every limitation of independent claims 1, 10, and 17, and this position underlies their challenge of all remaining dependent claims 2-9, 11-16, and 18-20.

Ground 1	Section 103	Obvious over Rockwood in view of Xie	Claims 1-20
-----------------	-------------	---	-------------

60. As discussed above, I apply the plain and ordinary meaning of all claim terms, including the district court’s clarifying comments, consistent with the district court’s claim construction order.

61. I disagree with the arguments in the Petition and the opinions set forth by Dr. Nielson for at least the reasons that I discuss in further detail below:

Petitioner's arguments based on the combination of Rockwood in view of Xie are unlikely to succeed because:

- (1) Rockwood does not disclose or render obvious “*gathering an event defining an action of a first object acting on a target*” “or “*the first object is executed on a device,*” because (a) POSITA would not understand an operating system or network layer as a “first object” and (b) Rockwood does not teach or render obvious gathering an event from endpoints about object actions on or within endpoints; (c) Rockwood does not disclose or render obvious collecting event information that includes whether an object was executed on a device;
- (2) Rockwood in view of Xie does not disclose or render obvious “*generating contextual state information for the event by relating the event to an originating object of the first object*” because Petitioner does not identify any disclosure of the claimed originating object, since information about objects on an endpoint is never collected;
- (3) a POSITA would not be motivated to combine Rockwood and Xie to practice this limitation since Rockwood and Xie embody the prior art problems identified by the '224 patent;
- (4) Rockwood in view of Xie does not disclose or render obvious “*obtaining a global perspective for the event based on the contextual state information, wherein the global perspective comprises information associated with one or more of the*

first object and the originating object, and wherein the global perspective relates to one or more other events related to the event across a network” because Rockwood’s “global view” is of the entire *system*, not for a particular monitored *event*, and the “global view” does not contain the required fields of information for the global perspective, *i.e.*, “*information associated with one or more of the first object and the originating object*” or “*one or more events related to the events across a network,*” and petitioner does not address this deficiency or supplement its argument with any citation to teachings from Xie; and

- (5) Rockwood in view of Xie does not disclose or render obvious “*generating 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*” because there is no disclosure in Rockwood or Xie of an event line that includes the fields of information required by the claims.

A. Rockwood’s Does Not Gather Information about Objects Acting on Targets or Executing on Devices

62. Claim limitations 1[b], 10[g], and 17[g] each require gathering an event defining an action of a first object. (EX-1001, cls. 1, 10, 17.) Claim 1[b] includes the additional limitation “*wherein the first object is executed on a device.*” Petitioner relies only on Rockwood for these limitations. (See Petition 14-17.) Petitioner’s

grounds do not disclose or render obvious these limitations because Rockwood does not gather event information about an object acting on a target or executing on a device.

Claim Limitation	Claim Language
1[b]	<i>“gathering an event defining an action of a first object acting on a target, wherein the first object is executed on a device.”</i>
10[b]	<i>“gather an event defining an action of a first object acting on a target”</i>
17[g]	<i>“gather an event defining an action of a first object acting on a target”</i>

1. The “Network Layer/OS” Is Not a “First Object”

63. Petitioner and its expert assert that Rockwood’s operating system/network teaches the claimed “first object.” (Petition 14, 17, 21, 29, 56.) Petitioner is wrong because a POSITA would not understand a network layer or operating system to be a “first object.” Petitioner fails to identify any support from the ’224 patent for the assertion that the “first object” may be an operating system or network layer. Indeed, Petitioner’s argument is incompatible with the ’224 patent, which describes the “first object” as an object that is “originated” by another object. Specifically, the ’224 patent requires determining the *originating object of the first object* in order to generate contextual state information. (See EX-1001 Claim 1[c]; see also Section V.A, *supra*.)

64. Petitioner does not identify any disclosure in Rockwood (or anywhere else in the prior art) of an originating object of an operating system or network layer. Instead, Petitioner argues that the originating object is Rockwood’s “attacker profile.” (Petition 17 (“Rockwood discloses a correlation engine that correlates detected events (e.g., attacks) from a source (e.g., OS such as UNIX with network layer, or source IP address) with source of the attack, embodied as an attacker profile or originating malware (‘originating object’)”); *see also id.* at 17-18 (“A PHOSITA would have recognized that the sources of attacks or originating malware (corresponding to ‘originating object of the first object’) corresponding to detected events would be generating events/attacks to be transmitted via the network layer/OS (‘first object’).”). But the attacker profile is generated by Rockwood and is *not* an operating system or network layer. Petitioner’s theory is nonsensical because it would require the operating system or network layer to have been originated by the “source of attacks or originating malware.” (*See* Petition 17-18.) This is wrong and also inconsistent with Dr. Nielson’s description of malware: “Malware is harmful application software (e.g., a process) that generates unwanted network traffic and causes the network layer to transmit it.” (EX-1002 ¶ 168; *see also* ¶ 72 (“‘Malware’ is the generic term given to all software that causes harmful (or unauthorized at the very least) operations to a victim’s computing systems. ‘Malicious software, also known as malware, refers to any software designed to infiltrate or damage a computer

system without the owner's informed consent.'.) A POSITA would not understand a network layer or operating system as "unwanted network traffic." Thus, Dr. Nielson's definition of malware further supports that a POSITA would not understand that a "source of attack or originating malware" could be an originating object of a computer's network layer or operating system.

65. Claim 8 further illustrates why neither the network layer nor the operating system satisfy the "first object" limitation. In claim 8, the claimed "global perspective" includes "a determination as to whether the first object is malware." (EX-1001 cl. 8, 4:54-61; 5:11-18). A POSITA would understand that neither an operating system nor a network layer would be considered as "malware," particularly in view of how this term is used in the claim 8.

66. Petitioner's expert, Dr. Nielson, acknowledges the problem with classifying the network layer and/or operating system as the claimed "first object acting on a target" in his declaration. He notes that "the network layer does not generate the data contents of the network transmission, it simply transmits whatever data is sent to it by application software (e.g., malware). In effect, the OS is somewhat like a mailroom, providing packaging, addressing, and transmission services. But the contents within the packages are given to it." (EX-1002 ¶171.) This concession that the network layer/operating system is simply the mailroom that "transmits whatever

data is sent to it by application software” further supports my opinion that the network layer/OS cannot be the claimed “first object acting on a target” because this admits that the executable application software, not the operating system or network layer, would be the computer object that acts on the target according to Petitioner’s theory.

67. Petitioner’s first argument that the “first object” is the network layer and/or operating system is thus wrong and should be rejected for all limitations for which petitioner relies on this mapping. (*See* Petition 14, 17, 21-22, 29, 38, 39, 46, 55-56, 60, 66.)

2. Rockwood Does Not Disclose or Render Obvious an Event Defining a First Object Acting on a Target

68. As discussed in the preceding section, Petitioner’s argument that a network layer or operating system can be a “first object” should be rejected. *See* Section VII.A.2, *supra*. With respect to petitioner’s second argument, Petitioner fails to identify any disclosure or teaching of a “first object” “acting on a target.” Rather, Petitioner conflates transmission of an executable file with the execution of the first computer object to act on a target. Specifically, Petitioner argues that Rockwood “discloses detecting and recording characteristics of an event (corresponding to ‘gathering an event defining...’), including a transmitting source of an event and a destination IP address (corresponding to a “target”) in which the data/code package

(corresponding to ‘first object’) is transmitted and executed on a network computer (corresponding to ‘executed on a device.’).” Based on this, Petitioner argues that the “event attributes relating to the package (e.g., malware) transmission and its effect/action on a target (corresponding to “event defining an action...”) are collected by the system of Rockwood.” Petition 16 (citing EX-1004 3:50-60, 12:35-45 and EX-1002 ¶¶159-163.) In other words, Petitioner argues that transmitting executable malware is the same as collecting an event relating to the execution of malware.

69. None of the Rockwood excerpts that Petitioner and its expert rely on relate to, much less disclose, an object *acting* on a target. Petitioner’s first citation describes the operation of network edge sensors which “may use algorithms, signatures, scripts, or any suitable detection or comparison technique to process packet headers, packet payloads, and/or any other data.” This information about Rockwood’s sensors does not disclose or render obvious gathering an event based on *an action of a first object acting on a target*.

70. Likewise, Petitioner’s second citation relates to detecting an “enemy hacker” attempting to hack into the system. (EX-1004 12:35-45 (“In the present example, an enemy attacker attempts to hack into system 10 to obtain sensitive information about supply levels tracked by system 10. System 10 detects this attack as detected event 110, which occurred at 5:20 p.m. and originated from a UNIX-based

computer. Detected event 110f contains a segment of code signifying that detected event 110f is an attack. Operator 60 of system 10 wants to determine whether any detected events 110 in detected event storage 158 may be related to this attack.”). But this does not discuss an *action of a first object acting on a target*. Instead, this discusses Rockwood’s system detecting an attack *event* and the computer from which it originated, but it does not identify a first *object acting on a target*. The intercepted data/code package is merely transmitted to the target computer; nowhere does Rockwood disclose that the data/code package mapped as the first object acts on the target computer. (See EX-1004 Fig. 3 (illustrating “a table of event information,” which does not include the computer object’s action or an identification of any computer object acting on a target).) Moreover, a POSITA would understand the intercepted information that Petitioner maps for this limitation regarding the transmission of an executable computer object does not imply that the executable computer object was ever, in fact, executed such that it acted on a target. It is possible that an executable computer object is transmitted but never executed, and one cannot assume an executable computer object has acted on a target without more information, such as a disclosure of it, in fact, acting on a target or information that it would automatically execute upon arrival at its destination.

B. The Rockwood-Xie Combination Does not Disclose or Render Obvious the “Originating Object”

71. Claim limitations 1[c], 10[h], and 17[h] each require generating contextual state information for an event by correlating the event to an originating object of the first object. (EX-1001, cls. 1, 10, 17.)

72. The petition does disclose or render obvious claim limitations 1[c], 10[h], and 17[h] because Rockwood-Xie does not disclose or render obvious the “originating object” required to generate contextual state information.

Claim Limitation	Claim Language
1[c]	<i>“generating contextual state information for the event by correlating the event to an originating object of the first object”</i>
10[h]	<i>“generate contextual state information for the event by correlating the event to an originating object of the first object”</i>
17[h]	<i>“determine a global perspective for the event based on the contextual state information for the event...wherein the contextual state comprises an indication of an originating object of the first object...”</i>

73. The petition does not identify any disclosure from the Rockwood-Xie combination of the claimed “originating object.” As explained by the ’224 patent, the originating object is the parent object, *i.e.*, the object that originated the first object. (EX-1001 Abstract (“The object, the event, and the target are then *correlated to at least one originating object such that an audit trail for each individual event is created.*”) (emphasis added).)

74. The petition asserts (in both its first and second mappings) that the originating object to Rockwood’s “attacker profile” as modified by Xie’s identification of infected hosts on a network based on detected changes to file attributes. (Petition 17 (“Rockwood and Xie disclose using an attacker profile to correlate an event to an originating object/process of the first object (e.g., originating malware or source) of an attack”); 19 (“originating object (e.g., attacker profile with originating malware information as in Xie”); *see also* EX-1005 30-32, 47-49). This is wrong because neither Rockwood nor Xie disclose an *originating object of the first object* being correlated to an event.

75. Petitioner and its expert suggest that the attacker profile, as modified by Xie, could be an originating object. (Petition 17-19; EX-1002 167.) Rockwood’s attacker profile cannot be the originating object because the attacker profile is not a parent object to the first object, nor is it described as a computer *object* that originates computer objects. Rather, Rockwood’s attacker profile “comprises a plurality of characteristics of an attacker of an enterprise’s computer network. In certain embodiments, existing attacker profile 224a includes name and background information such as, for example, last known residence or last known employer.” (EX-1004 10:8-22). The attacker profile is a collection of information about a person or entity that is attacking the network—it is not an originating object. Indeed, Petitioner fails to

identify any disclosure or teaching of the attacker profile acting to create a child “first object.”

76. Petitioner attempts to address these shortcomings by arguing that “Xie teaches identifying originating malware of an attack (‘originating object’).” (Petition 18). This is wrong. The passages from Xie on which Petition relies teach identifying *hosts* on a network that have been infected by malware using information about changes to file attributes. (EX-1005 30-32, 47-49). There is no teaching (and petitioner does not cite any) of an identification of an *originating object* of the first object, or the identification of parent/child relationships between computer objects.

77. Petitioner misplaced reliance on Xie’s “anomaly detection” system “that uses file system updates to represent host state changes for anomaly detection” is misplaced. (EX-1005 31-32; 47-49). Xie discusses the testing of its prototype system “Seurat” using a Lion worm in order to trace the propagation of that worm across hosts on a network. (EX-1005 47-49, Figure 2.12). Seurat’s intrusion detection is depicted in Figure 2.12:

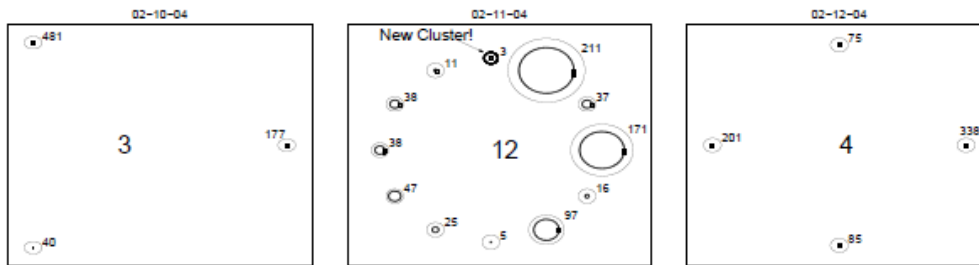


Figure 2.12: Intrusion detection by Seurat. Seurat identified a new cluster of three hosts on Feb 11, 2004, when we manually launched the Lion worm. The number of clusters formed in each day varies due to an artifact of the feature vector selection and the clustering algorithm.

(EX-1005 48 Fig. 2.12)

78. Xie does not disclose or teach identifying computer objects as malware, or even any audit trail of the lineage of *computer objects*. Rather, Xie discusses identifying the infected *hosts* with information about file system changes, such as to their file size. (EX-1005 47-49.) Xie and its prototype, Seurat, do not use this information to identify an originating *object*, or malware objects. This is confirmed by Xie’s discussion of how human administrators—not Seurat—may use information about file system changes to identify the root cause of the file system changes. (EX-1005 48.) As Xie notes, during testing “Seurat successfully detects a new cluster consisting of the 3 infected hosts. Figure 2.13 lists the 22 files selected by Seurat as the causes of the alarm. These files provide enough hints to the administrators to confirm the existence of the Lion worm.” (EX-1005 48 (emphasis added); *see also* 33 (“For each alarm, Seurat identifies the list of hosts involved and the related files,

which we expect will be extremely helpful for system administrators to examine the root cause and dismiss false alarms.”). Since Xie merely teaches providing *hints* that could be helpful to an administrator attempting to identify the Lion worm, and the burden is on the *administrator* to interpret the hints to identify the Lion worm, clearly Xie does not identify the Lion worm. Petitioner and its expert fail to explain how these hints provided to a system administrator regarding an infected *host* disclose or render obvious limitations 1[c], 10[h], and 17[h] “originating object.”

79. Petitioner and its expert suggest that Xie teaches identification of the Lion worm (Petition 18 (“Xie discloses identifying the identify/name and location of the originating malware (e.g., Lion worm)”); *see* EX-1002 ¶¶177, 218 (“Rockwood in view of Xie discloses identifying the originating object/malware and including that information in Rockwood’s attacker profile”)), but that is a mischaracterization of Xie. In Xie, the Lion worm was selected by Xie’s authors as the version of malware to be used for testing the Seurat prototype. (EX-1005 47 (“The Lion worm was found in early 2001 We configured the isolated cluster with three Lion vulnerable hosts and one additional machine that launched the worm.”) (emphasis added).) Petitioner and its expert’s argument that Xie discloses identifying the originating malware is dependent on the fact that the identity of the originating malware—in the case of Xie, the Lion worm—is already known. Thus, Xie does not

determine whether the Lion worm has originated another computer object. Rather, Xie looks for the Lion worm specifically for purposes of testing the Seurat prototype—without regard to information about its familial relationships. Petitioner and its expert do not identify any disclosure of Xie determining the Lion worm from which any subsequent Lion worm originated.

80. Xie’s file change monitoring does not disclose or render obvious identifying parent/child relationships between computer objects. Indeed, Petitioner and its expert do not identify any disclosure from Xie (or Rockwood) discussing identifying, analyzing, or attempting to determine a parent-child relationship between computer objects. (*See generally* Petition; EX-1002.) Thus, even if Xie could be described as identifying a potentially suspicious file based on file system changes, it still does not analyze or identify the parentage of computer objects.

81. Petitioner fails to address these critical deficiencies or otherwise explain how Rockwood’s attacker profile, which is not described as an executable and does not perform any action, can be an “originating object”, or how Xie determines parent child relationships for purposes of identifying an originating object of a first object.

82. Given these failures, Petitioner’s proposed combination for this limitation, i.e., “include[ing] the file change correlations of Xie with the correlations of

Rockwood and include Xie’s originating malware information in Rockwood’s attacker profile” (Petition 19) fails to disclose or render obvious the claims’ “originating object.”

83. Accordingly, it is my opinion that the petition fails to establish a reasonable likelihood of success to show limitations 1[c], 10[h], and 17[h] are disclosed or rendered obvious by Rockwood in view of Xie.

C. POSITA Would Not Have Been Motivated to Combine Rockwood with Xie Because Each Reference Embodies the Problems of the Prior Art

84. Both Rockwood and Xie suffer from an inability to look inside the endpoints to collect contextual information around an observed event. *See* Sections V.A, *supra*. As discussed above, both Rockwood and Xie perform their respective network forensic analysis techniques using sensors placed along communication pathways to collect network traffic. *See* Section VI.A-B, *supra*. This shortcoming is an aspect that the ’224 patent was invented to address. (*See* EX-1001 (’224 patent) 1:36–51.) As explained by the ’224 patent’s descriptions of its advantages over the prior art:

However, existing network forensics tools, such as network sniffers and packet capturing tools, passively collect information about network traffic. Such tools may be able to detect and capture information associated with communication sessions, such

as hostnames, ports, protocols, IP addresses, etc.; however, such tools tend to receive network events outside of a host or system. That is, a network forensic tool, such as a network sniffer, may reside at a network edge and may receive network events concerning the network from one or more hosts or systems. Accordingly, network edge devices have no ability to establish any sort of context from within the host or system that is generating the event. Therefore, devices residing at a network edge may monitor, record, and or analyzes network traffic between the host and the device, but information that may be useful within the host is not obtained.

(See EX-1001 1:36–51.)

85. Neither Rockwood nor Xie collect information about an event from the host computers, and instead rely on intercepting network transmissions outside the host computers using sensors along the network’s communications pathways. As also discussed above, the Rockwood + Xie combination fails to identify or collect information about the “originating object” because it does not obtain information about computer objects’ actions from the host computer. *See* Section VII.B, *supra*. As a result, a PHOSITA would not have been motivated to combine Rockwood with Xie to attempt to practice the claims of the ’224 patent.

D. Rockwood Does Not Obtain a Global Perspective for the Event

86. Claim limitations 1[d], 10[i], and 17[h] each require obtaining a global perspective for an event based on the contextual state information, wherein the global perspective comprises information associated with one or more of the first object and the originating object, and wherein the global perspective relates to one or more other events relates to the event across a network. (EX-1001, cls. 1, 10, 17.)

Petitioner's grounds do not disclose or render obvious this limitation.

Claim Limitation	Claim Language
1[d]	<i>“obtaining a global perspective for the event based on the contextual state information, wherein the global perspective comprises information associated with one or more of the first object and the originating object, and wherein the global perspective relates to one or more other events related to the event across a network”</i>
10[i]	<i>“obtain a global perspective for the event based on the contextual state information, wherein the global perspective comprises information associated with one or more of the first object and the originating object, and wherein the global perspective relates to one or more other events related to the event across a network”</i>
17[h]	<i>“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 wherein the contextual state comprises an indication of an originating 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”</i>

87. Rockwood does not disclose a “*global perspective for the event*” because Rockwood’s “global view,” which Petitioner cites as the “global perspective,” is for the *entire system*, and *not* for any given monitored event, (EX-1004 14:24-29 (“Global server 40 then processes detected events 110 and provides operator 60 with a global view of the state of system 10”) (emphasis added); 19:27-31 (“According to certain embodiments GUI 52p in network node 610p displays n-dimensional graphs 340p, 340q, 340r, and 340s to operator 60p of network node 610p. Thus, operator 60p obtains a more complete view of the state of system 10”) (emphasis added).) An event-based global perspective is an explicit claim requirement. (See, e.g., EX-1001 cls. 10[i] (“obtain a global perspective *for the event*”) (emphasis added); 17[h] (“determine a global perspective *for the event*.”).)

88. Petitioner appears to recognize this deficiency, arguing that “a PHOS-ITA would have understood that the network-level aggregation and global view in Rockwood based on the correlated data as modified by Xie teach the recited global perspective ‘wherein the global perspective relates to one or more other events related to the event across a network,’ as well as ‘wherein the global perspective comprises information associated with one or more of the first object and the originating object.’” Petition 23. This argument fails to explain how Rockwood’s network level

aggregation of information alongside its “global view” disclose or render obvious the claimed “global perspective.”

89. First, Rockwood uses the term “global view” *once*, but does not disclose how the global view is generated, what it includes, and what it relates to. (EX-1004 14:29.) As a result, there is no disclosure or teaching that the global view is obtained based on the contextual state, no disclosure that the global view includes information associated with the first object or originating object, and no disclosure that the global view relates to *events* related to the event across a network. Petitioner’s reliance on Rockwood’s “global view” is vague and misplaced, because it fails to address why or explain how a POSITA would understand Rockwood’s network-level aggregation of information to disclose or render obvious the claimed “global perspective.”

90. Thus, it is my opinion that the petition does not disclose or render obvious limitations 1[d], 10[i], and 17[h].

E. Rockwood in View of Xie does Not Disclose or Render Obvious an Event Line Comprising Information Relating to the Event

91. Claim limitations 1[e], 10[j], and 17[i] each require generating 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. (EX-1001, cls. 1, 10, 17.) The petition does not disclose or render obvious these limitations.

Claim Limitation	Claim Language
1[e]	<i>“generating an event line comprising information relating to the event, wherein the information relates to at least one of the first object, the actions of the first object, the target, and the originating object”</i>
10[j]	<i>“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”</i>
17[i]	<i>“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”</i>

92. The petition does not identify any disclosure from the combination of Xie and Rockwood of an *“event line”* with at least one of the required fields of information, i.e., relating *“to the first object, the action of the first object, the target, or the originating object.”*

93. Instead, Petitioner maps the event line to Rockwood’s display of an attacker profile on a graphical user interface. (Petition 23-25.) But the information Petitioner points to in Rockwood’s attacker profile does not include the requisite information for the claimed event line. (Petition 24 (citing EX-1004 4:48-51, 7:3-10, 7:20-22, 10:34-44, 16:62-66).) Petitioner and its expert suggest that information about source or destination IP addresses could constitute one of information about

the “*first object, the action of the first object, the target², and the originating object*” is incorrect because that information relates to the particular endpoint, not the particular *objects* relating to the event. And, as discussed earlier, Rockwood collects information using sensors that capture transmissions between nodes, and does not include information reflecting the *actions* of a computer object—only the transmission of a computer object. (See Section VI.A, *supra*.)

94. Critically, Rockwood’s attacker profile cannot be the claimed event line because it is a profile about characteristics of an *individual attacker*. (EX-1004 4-22 (“[C]orrelation engine 140 is operable to generate a new attacker profile 224b based on the event information of identified detected events 222. Each existing attacker profile 224a comprises a plurality of characteristics of an attacker of an enterprise’s computer network. In certain embodiments, existing attacker profile 224a includes name and background information Such as, for example, last known residence or

² “Target” is used in both Rockwood and the ’224 patent, but in different non-overlapping ways. In the ’224 patent, “target” refers to “information and/or details describing *the object or identity of another entity upon which the act is being performed* (the ‘Victim’ or ‘Target’).” (EX-1001 7:48-51). The ’224 patent thus requires the target to be object or entity acted upon, but petitioner does not identify any disclosure from Rockwood of a computer object executing or acting upon another computer object, and instead relies on the mere possibility that a detected transmission could include an executable file. See Section V.A, *supra*. By contrast, Rockwood’s target is “an event selected or defined by operator 60 to serve as the basis for correlating detected events 110 in detected event storage” (EX-1004 7:3-5.).

last known employer. For example, a particular existing attacker profile 224a may correspond to an individual who typically launches attacks between 5:00 p.m. and 5:30 p.m. using external computers with IP addresses between 205.252.48.160 and 205.252.48.200. These characteristics are included in existing attacker profile 224.a for this individual. By determining the identity of an attacker, operator 60 may be able to preempt future attacks.”)

95. Petitioner contends that “Rockwood and Xie also disclose ‘wherein the information relates to at least one of the first object, the action of the first object, the target, and the originating object’ for the reasons discussed above for limitations 1[b] and 1[c]” by pointing to various types of information, such as OS information, IP address of source device, etc. (Petition at 24-25.) However, Petitioner does not identify any such disclosure showing, or explaining how, any of the information would be displayed on Rockwood’s GUI display of an attacker profile—which relates to the individual responsible for an attack—could be modified to display an *event line* with the fields of information required by the claims. And Xie does not disclose or render obvious a GUI that displays the fields of information required by the claims.

96. To use a simple analogy: Petitioner proposes using the teachings of Rockwood and Xie to modify a profile for an individual’s personal social media into an e-vite format relating to an event, notwithstanding the absence of any disclosure

or teaching from Xie or Rockwood regarding how to format an e-vite or incorporate the fields of information necessary for an e-vite. It would not have been obvious to POSITA to modify the format, such as a social media profile or attacker profile, so that it instead included the fields of information that would make it an event as claimed by the '224 patent, or e-vite in the context of this analogy. Petitioner and its expert Dr. Nielson do not explain how to actually modify the attacker profile relating to an individual attacker, or its presentation on the GUI, so that it instead includes the event information required by claim limitations 1[e], 10[j], and 17[i].

97. Based on the foregoing, it is my opinion that Petitioner fails show that Rockwood in view of Xie discloses or renders obvious limitations 1[e], 10[j], and 17[i].

F. Dependent Claims

98. Because Rockwood in view of Xie does not render obvious all limitations of independent claims 1, 10, and 17, I understand that Ground 1 fails to render obvious dependent claims 2-9, 11-16, and 18-20 as well.

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

99. It is my understanding that this declaration is being provided in support of Patent Owner's Preliminary Response. I have provided analysis of key limitations not included in the prior art. The fact that I have not analyzed 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.

IX. SECONDARY OBJECTIVE INDICIA OF NONOBVIOUSNESS

100. I understand that in determining obviousness of a 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. I further understand that these indicia constitute independent evidence of nonobviousness that can be the most probative in that regarding “in avoiding the trap of hindsight when reviewing, what otherwise seems like, a combination of known elements.”

101. As discussed by my summary of the prior art above, there was at least a long-felt and persistent need prior to the '224 patent to improve upon existing forensic malware mitigation techniques that failed to include useful context from within each endpoint. (*See* Section V, *supra*.) Prior attempts to develop such methods were limited by the use of network edge devices that may have intercepted data transmissions along communication pathways but otherwise failed to include useful information about a computer objects activities within an endpoint. (*See* Section IV, *supra*.) Where others failed, the '224 patent succeeded. (*See* Sections IV-VI, *supra*.)

102. Patent Owner currently accuses at least four industry participants, including Petitioner, of infringing the technology claimed in the '224 patent, demonstrating the critical need and widespread industry reliance on these novel methods. (*See* EX-2017; *See* EX-2015; *See* EX-2016; *See* EX-2018.) Petitioner, in particular, markets and provides Trend Micro's XDR technology, the components of which practice the systems and methods claimed in the '224 patent. (*See* EX-2017.)

103. These secondary indicia further support my opinion that the '224 patent was nonobvious.

X. CONCLUSION

104. For at least the foregoing reasons, it is my opinion that Petitioner's ground does not render obvious any of the challenged claims of the '224 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 17th day of July, 2023 in Los Angeles

Respectfully submitted,



Nenad Medvidovic, Ph.D.