UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Sophos Ltd. and Sophos Inc.,
Petitioners

v.

Webroot Inc.,
Patent Owner.

Case No. IPR2023-00731

U.S. Patent No. 8,201,243

Declaration of Dr. Henry Houh
In Support of Petitioners in the
Petition for *Inter Partes* Review of U.S. Patent No. 8,201,243

Mail Stop **PATENT BOARD**
Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

TABLE OF EXHIBITS

Exhibit Number	Document
1001	U.S. Patent No. 8,201,243 ("the '243 Patent")
1002	File History of the '243 Patent
1003	Reserved
1004	Curriculum Vitae of Dr. Henry Houh
1005	Li, et al., *UCLog: A Unified, Correlated Logging Architecture for Intrusion Detection*, Int'l Conf. on Telecomm. Sys.-Modelling & Analysis (2004) ("Li")
1006	U.S. Patent No. 8,117,659 ("Hartrell")
1007	Salvador Mandujano Vergara, *A multiagent approach to outbound intrusion detection* (2004) (Ph.D. Thesis, Instituto Tecnológico y de Estudios Superires de Monterrey) (on file with Repositorio Institucional del Tecnológico de Monterrey (RITEC) in the Instituto Tecnológico y de Estudios Superiores de Monterrey Library) ("Mandujano")
1008	U.S. Patent No. 7,174,566 to Yadav ("Yadav")
1009	Declaration of Dr. Sylvia D. Hall-Ellis
1010	Reserved
1011	Jeff Crume, *Inside Internet Security: What Hackers Don't Want You to Know* (Pearson Educ. Ltd. 2000)
1012	Information Sciences Institute, Univ. of S. Cal., *Internet Protocol: DARPA Internet Program Protocol Specification* (1981)
1013	Reserved

Exhibit Number	Document
1014	Reserved
1015	Mandia, K. & Prosise, C., *Incident Response: Investigating Computer Crime* 2001

TABLE OF CONTENTS

Page

I. INTRODUCTION 1

II. BASIS FOR OPINIONS 2

A. Qualifications 2
B. Preparation for This Declaration 13

III. LEGAL STANDARDS 13

A. A Person of Ordinary Skill in the Art 13
B. Legal Standard for Prior Art 15
C. Claim Construction 16
D. Legal Standard for Obviousness 17

IV. TECHNOLOGY BACKGROUND 19

A. Overview of Malware 19
B. Overview of Malware-Detection Software 22
C. State of the Art 22

V. THE '243 PATENT 23

A. Overview of the '243 Patent 23
B. Overview of the Challenged Claims 27

VI. PRIOR ART CONSIDERED 27

A. Identification of the Primary Prior-Art References 28
B. General Overview of the Primary Prior-Art References 29

VII. ANALYSIS OF THE CHALLENGED CLAIMS AGAINST THE PRIOR ART 33

A. Claim Construction 33
B. Application of the Prior Art to the Claims 34
C. Ground 1: Li in View of Hartrell Renders Obvious Claims 1-14 34
D. Ground 2: Li in View of Hartrell and Mandujano Renders Obvious Claims 1-14 77
E. Ground 3: Claims 1-14 are obvious under §103 over Li and Yadav. 87
F. Ground 4: Claims 1-14 are obvious under §103 over Li and Yadav, and Mandujano. 103

VIII. SECONDARY CONSIDERATIONS 105

IX. RIGHT TO SUPPLEMENT 105
X. CONCLUSION 107

I. INTRODUCTION

1. I, Dr. Henry Houh, have been retained by Gibson, Dunn & Crutcher LLP on behalf of Sophos Ltd. and Sophos Inc. ("Petitioners") as an independent expert in this Petition for *inter partes* review ("IPR") by the U.S. Patent and Trademark Office. I have been asked to provide analysis and expert opinions on U.S. Patent No. 8,201,243 ("the '243 Patent"), and, in particular, the validity of Claims 1-14 ("the Challenged Claims").

2. In my view, the Challenged Claims of the '243 Patent are invalid over the prior art I discuss in this Declaration. My opinion is that the prior art discloses the invention claimed in the Challenged Claims, so the Challenged Claims are invalid as obvious over the prior art.

3. I am being compensated for my work in this matter at my standard hourly rate. I am also being reimbursed for reasonable and customary expenses associated with my work and testimony in this proceeding. My compensation is not contingent on the outcome of this matter or the specifics of my testimony.

4. Based upon the facts and information available to me to date, I will detail my opinions that are relevant to this petition for IPR. I am prepared to provide expert testimony on the opinions I express if asked about those issues by the Board or others.

5. In this Declaration I discuss my own work, teachings, and knowledge of the state of the art in the relevant time period, and I cite technical literature (like handbooks and textbooks) to demonstrate the state of the art in the relevant period.

6. Throughout this declaration, I refer to specific line numbers or page numbers of the relevant prior art or other technical documents. Those citations might not be exhaustive—there may be more evidence to support a particular proposition than I cite here in this Declaration.

II. BASIS FOR OPINIONS

A. Qualifications

7. The details of my background and education, and a listing of all publications that I have authored, are provided in my Curriculum Vitae, a copy of which is submitted as EX-1004. The following is a brief summary of my relevant qualifications and professional experience.

8. I received a Ph.D. in Electrical Engineering and Computer Science from the Massachusetts Institute of Technology ("MIT") in 1998. I also received a Master of Science degree in Electrical Engineering and Computer Science in 1991, a Bachelor of Science Degree in Electrical Engineering and Computer Science in 1989, and a Bachelor of Science Degree in Physics in 1990, all from MIT.

9. During my college studies, I focused on communications and data networking. I took specialized courses including graduate courses in telecommunications networks, optical communications, and data networking. I, along with other graduate students in a networking research group, maintained both the computer workstations and the networking devices in the research group.

10. I have worked in data networking, data monitoring, and distributed networking systems on several occasions. As part of my doctoral research at MIT from 1991-1998, I worked as a research assistant in the Telemedia Network Systems ("TNS") group at the Laboratory for Computer Science. The TNS group built a high-speed gigabit ATM network and applications which ran over the network, such as remote video capture (including audio), processing and display on computer terminals. In addition to helping design the core network components (such as the ATM switch), designing and building the high-speed ATM links, and designing and writing the device drivers for the interface cards, I also set up the group's web server, which at the time was one of the first several hundred web servers in existence. I also set up log monitoring and data analysis systems on the web server.

11. Like all ATM networks, interconnection of various endpoints in our ATM system required the setup of end-to-end virtual circuits which required, for each ATM switch in the connection path, the switch's header remapping tables to be

configured for each virtual circuit required. I developed and implemented our system's protocol of controlling the content of these tables and the overall circuit setup, by monitoring the data network for specialized connection setup cells.

12. The TNS group was the first group to initiate a remote video display over the World Wide Web. Vice President Al Gore visited our group in 1996 and received a demonstration of—and remotely drove—a radio-controlled toy car with a wireless video camera mounted on it; the video was encoded by TNS-designed hardware, streamed over the TNS-designed network and displayed using TNS-designed software.

13. I authored or co-authored 12 papers and conference presentations on our group's research. I also co-edited the final report of the gigabit networking research effort with Professor David Tennenhouse and Senior Research Scientist David Clark. David Clark is generally considered to be one of the fathers of the Internet Protocol and served as Chief Protocol Architect for the Internet. With its focus on networking, the group, including myself, set up and maintained the network and computer systems. These systems included the networking on the workstations and desktops, the distributed file system, desktops and workstations, setting up and maintaining the distributed file system (Network File System) and the authentication system (Network Information Service, formerly known as Yellow Pages).

14. I defended and submitted my Ph.D. thesis, titled "Designing Networks for Tomorrow's Traffic," in January 1998. As part of my thesis research, I analyzed local-area and wide-area flows to show a more efficient method for routing packets in a network, based on traffic patterns at the time. My thesis involved capturing and analyzing flows of data in the network and the routing efficiencies gained by labeling the flows at the edge of the network, and routing the data based on the label instead of the IP destination address. My analysis included different methods of setting up the granularity of the flows for the most efficient use of routing resources. This type of label switching became popular with Multiprotocol Label Switching (MPLS) later implemented in various commercial routers. I gathered a large amount of network traffic, used publicly available network traces, and broke the traffic into different types of flows using various parameters for classifying the flows. My thesis also addressed real-time streamed audio and video. The network traffic that I analyzed was IP protocol traffic, including UDP and TCP. During this time, I also investigated and utilized network security tools to identify vulnerabilities in computer systems.

15. I have been involved in Voice over Internet Protocol ("VoIP") data streaming technologies since 1997 and have specific experience in designing, monitoring, and testing VoIP networks.

16. From 1997 to 1999, I worked at NBX Corporation, which was acquired by 3Com Corporation in 1999. During this time, I was a Senior Scientist and Engineer working in IP Telephony. NBX delivered the world's first fully featured business telephone system to run over a data network, the NBX100. NBX was one of the first business phone systems to be configurable via a web interface. Users and administrators had access to varying levels of configuration for the phone system.

17. As part of my work at NBX, I designed the core audio reconstruction algorithms for the telephones which depacketized the voice data and reconstructed the audio. In addition, I designed the voice data packet transmission algorithms. I also created a system to capture and log network packets sent by devices in the NBX system for monitoring, testing, and debugging. The system analyzed the packet log while linking data from distinct packets in order to identify problems and errors within the system. I also designed and validated the core packet transport protocol used by the phone system. In addition, I designed and oversaw the development of the underlying transport protocol used by the NBX100 phone system for reliable packet transport. That transport protocol is still used by the NBX100 system and its successors and is estimated to be used hundreds of millions of times daily. I wrote NBX's first demonstration IP software stack, which added the capability for utilizing the NBX100 phone system on an IP network. I also specified and prototyped the

phone system's support for Differentiated Services. NBX first demonstrated a phone in the NBX100 system working over the Internet in 1998 at a trade show in Las Vegas, for which I acquired, set up, and configured Virtual Private Network tunnels to carry the traffic. I was later the lead architect in designing NBX's next-generation highly scalable system. After NBX was acquired by 3Com, I did some work with 3Com's cable equipment division, including demonstrating a working NBX IP phone system over 3Com's cable equipment infrastructure using an early version of DOCSIS at a trade show in 1999. The NBX100 was the market's leading business phone system to run on a data network for several years following its introduction. During that time, I became more familiar with the various standards relevant to Internet telephony as well as the problems with which designers of commercial telephony operations were faced in implementing VoIP.

18. I, along with two of NBX's founders, was awarded U.S. Patent No. 6,967,963 titled "Telecommunication Method for Ensuring On-Time Delivery of Packets Containing Time-Sensitive Data," for some of the work we did while at NBX.

19. After NBX, I worked at Teradyne, a test tool company primarily focused on semiconductors. Teradyne had recently acquired Hammer, a company that specialized in load and functional testing for telecommunications systems. The

Hammer product is well known as a telecom test, measurement, and monitoring tool. Teradyne spun out Hammer and several other internal divisions into an independent company called Empirix. I became Chief Technologist of the Hammer division of Empirix. Empirix was a leader in VoIP network testing and monitoring. The Hammer was also used by the Empirix business units to provide testing and monitoring of interactive voice response units and call centers. I worked with members of this business units on some projects and we received U.S. Patent No. 7,590,542, titled "Method of Generating Test Scripts Using a Voice-Capable Markup Language" for some of the work I did with them.

20. At Empirix, I laid out a new multi-year product vision for data network testing and monitoring, secured internal funding for the effort, and led a team to deliver a new technology platform to the market in February 2001. This new product, PacketSphere, initially emulated network behavior so that wide-area VoIP connections could be tested in a lab. A later release allowed PacketSphere to generate high volumes of VoIP calls, including media streams, and to monitor the quality of VoIP voice streams. PacketSphere was also used in the Storage Area Network area. Later, the core technology was added to other Empirix products such as Empirix's Hammer XMS to monitor thousands of VoIP media streams in real time to determine their quality. PacketSphere was Empirix's most successful new

platform introduction at the time. Companies purchased the PacketSphere product to emulate an Internet Protocol network to see the effects of deploying their product on the Internet prior to launch. PacketSphere received several industry awards.

21. In addition, I worked with the web testing business unit of Empirix on a number of new and upgraded products. I specified and prototyped a website security threat assessment tool, which we previewed with some potential customers and used to find security threats on their websites. We received U.S. Patent No. 7,975,296, titled "Automated security threat testing of web pages," for some of the work I did on this project. Empirix also provided the use of our web-testing tool as a service to companies, some of which used our tool to continuously monitor their websites for performance issues.

22. During my time at Empirix, I presented lectures on VoIP and data network testing and monitoring to companies including Lucent Labs (formerly AT&T Bell Labs). I was also invited to present several guest lectures in a software engineering course at MIT. Since then, I have also participated twice as a unit lecturer in an experimental course that was taught by an Institute Professor (the highest award that an MIT Professor can achieve) and sponsored by the Chairman of the MIT Corporation (MIT's board of trustees).

23. From 2004 to 2008, I was employed by BBN Technologies Corp., a technology research and development company located in Cambridge, Massachusetts. BBN Technologies is a world-renowned company with expertise in acoustics, speech recognition, and communications technology. BBN Technologies staff have pioneered many networking technologies and Internet applications and have built some of the world's largest government and commercial data networks.

24. My duties and responsibilities at BBN Technologies generally included commercialization of the technologies developed by BBN Technologies, which included spinning off companies and growing commercial businesses in-house. I worked on commercializing a service offered by BBN to monitor call centers and provide analytical data on each call. The system generated logs of every call into the system, analyzed each call for particular events, and highlighted those that may have suffered erroneous processing. The business became known as AVOKE Analytics and provided call center analytics for large organizations such as Dell and the Centers for Medicare and Medicaid Services (CMMS). For a time, during the rollout of the Affordable Care Act (though I was no longer working at BBN), AVOKE Analytics gathered data and provided call-by-call analytics for every call made to the CMMS main call center.

25. In addition, I was involved in utilizing the award-winning AVOKE STX speech recognition technology to create the public audio/video search engine EveryZing (formerly known as PodZinger) which was spun out into a stand-alone company now known as RAMP, Inc. PodZinger won the 2006 MITX Technology Award for best Web 2.0 Application and was also named the 2006 Forbes Favorite Video & Audio Search Engine, beating out Google, Yahoo, and other companies. After managing the creation of the initial prototype system, PodZinger built out a full streaming audio and video search solution when I was the Vice President of Operations and Technology there. I was also involved in the Boomerang Mobile Shooter Detection project as the Vice President of Engineering for the program. The Boomerang system was deployed to Iraq and Afghanistan and was credited with saving many lives.

26. I also worked with numerous other researchers at BBN with an eye towards possible commercialization of the technology. Among these projects included a zero-day security threat detection system for computers, semantic search, a body-area network technology, and ad-hoc networks. Some of BBN's threat detection technology involved utilizing a signature database to examine packets for polymorphic exploits, which are those that change over time and are particularly hard to detect.

27. In 2012, I opened Einstein's Workshop, a 7,000-square-foot facility for teaching science, technology, engineering, and math to children. I created courses, hired the staff, trained staff, and oversaw the financial management of the company, and provided approximately 300,000 student instruction hours in our STEM courses. We also created an educational 3D Computer-Aided Design program, which we spun-out into a separate company, BlocksCAD. BlocksCAD has received grants from DARPA DSO and the USDA and has participated in the LearnLaunch, MIT Play Labs, and MassChallenge accelerator programs. BlocksCAD currently has over 200,000 registered users and is used in schools throughout the U.S.

28. From 1989 to 1990, I worked at AT&T Bell Laboratories on optical computers. This work generated six peer-reviewed papers, and multiple U.S. and European patent applications in which I was named as a co-author or inventor. I also interned at AT&T Bell Laboratories in 1987 and 1988. Additional relevant experience in the field of computer networking is listed in my Curriculum Vitae.

29. I am a named inventor on several additional patents including: U.S. Patent No. 6,967,963, titled "Telecommunication Method for Ensuring On-Time Delivery of Packets Containing Time-Sensitive Data," U.S. Patent No. 7,801,910, titled "Method and apparatus for timed tagging of media content," U.S. Patent No. 9,697,231, titled "Methods and apparatus for providing virtual media channels based

on media search," and U.S. Patent No. 9,697,230, titled "Methods and apparatus for dynamic presentation of advertising, factual, and informational content using enhanced metadata in search-driven media applications."

B. Preparation for This Declaration

30. My findings contained in this declaration are based on my education, research, experience, and background in the fields of network computing and cybersecurity, as well as my review of prior-art references and other documents disclosed in this declaration. In forming my opinions, I have studied and considered the '243 Patent, the file history of the '243 Patent, the prior-art references cited in this Declaration, and the other references I cite or refer to in this report.

31. I understand that this declaration will be submitted in support of a Petition requesting IPR of the '243 Patent.

III. Legal Standards

32. Petitioner's counsel has told me about the following legal standards for this case, which I have adhered to and applied throughout my analysis.

A. A Person of Ordinary Skill in the Art

33. Petitioner's counsel has told me that a person of ordinary skill in the art, or a "POSITA," is a hypothetical person from whose viewpoint the prior art is analyzed (without the benefit of hindsight). A POSITA uses conventional wisdom

in the art but does not try to innovate, either by extraordinary insights or by systematic research.

34. Petitioner's counsel has also told me that the hypothetical POSITA has knowledge of all prior-art references that are sufficiently related to one another and to the pertinent art, and to know of all prior art in the fields reasonably pertinent to the particular problem that the claimed invention purports to address.

35. In evaluating the prior-art references and other material, I have used the perspective of a POSITA in the field to which the patent is related as of the time of the patent's priority date. I understand that a POSITA is presumed to be aware of all pertinent prior art and the conventional wisdom in the art and is a person of ordinary creativity. I have applied this standard in my analysis throughout my declaration.

36. The '243 Patent is entitled "Backwards Researching Activity Indicative of Pestware." Counsel for the Petitioners have told me that the 2006 timeframe is the earliest claimed effective filing date of the '243 Patent, and a POSITA at that time would have had at least a Bachelor's degree in Computer Science, Computer Engineering, Electrical Engineering, or an equivalent discipline, and at least two years' worth of experience developing computer networking or network architecture, or a Master's degree in a related field. Or, instead of the education

requirements, more education could substitute for less work experience and vice versa. Additionally, a POSITA would either have six months' experience as a network or system administrator, or have taken two advanced computer-security courses. A POSITA would have been familiar with at least the fields of computer networking, operating-system design, and distributed systems.

37. I have met the criteria described above since long before 2006, so I would have been a POSITA with regard to the '243 Patent at the time of the earliest priority date Patent Owner claims for the '243 Patent.

B. <u>Legal Standard for Prior Art</u>

38. Petitioner's counsel has told me that a patent, published patent application, or other publication, must first qualify as prior art before it can be used to invalidate a patent claim.

39. Counsel has told me that a U.S. or foreign patent qualifies as prior art to a patent claim if the date of application, issuance, or publication of the prior-art patent is before the purported date of invention of the patent claim.

40. Counsel has also told me that a printed publication (like a technical publication, a magazine article, or newsgroup post) qualifies as prior art to a patent claim if the date of publication is before the purported date of invention of the patent claim. Counsel has also told me that a U.S. patent qualifies as prior art to a patent

claim if the application for the prior-art patent was filed in the United States before the purported date of invention of the patent claim. Finally, Counsel has told me that, if a U.S. Patent incorporates another patent or document by reference, it is considered to be part of that same reference.

C. Claim Construction

41. Counsel have told me that in an IPR, the Board uses the same standard for construing the challenged claims as during claim construction in district court civil actions. Counsel have also told me that, in the district court context and in this IPR, the words of a claim are generally given their ordinary and customary meaning—that is, the meaning a term would have to a person of ordinary skill in the relevant art at the time of the invention. The time of invention is generally the time the application was filed, or, as is the case here, the filing or effective date of the application to which a patent claims priority; which here is April 20, 2006, for the '243 Patent. Accordingly, I have used April 2006 for my analysis in this Declaration. Counsel have also told me that the specification informs the proper interpretation of a claim. This is because a POSITA is assumed to have read the claim term not only in the context of the particular claim in which the disputed term appears, but in the context of the entire patent, including the specification. Counsel have also told me that the prosecution history and extrinsic evidence concerning relevant scientific

principles, the meaning of technical terms, and the state of the art are also considered in ascertaining the meaning of claim terms.

D. Legal Standard for Obviousness

42. Counsel has told me that an invention may be obvious, even if it is not identically disclosed or described in a single prior-art reference, as long as the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious to a POSITA at the time the invention was made.

43. Counsel has also told me that the Supreme Court has told the PTO to be cautious about granting a patent based on the combination of elements found in prior art, because a patent for a design that only combines old elements but does not actually change their respective functions removes an already-known design from the public and gives it exclusively to the patentee. The combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results.

44. Counsel has also told me that when a work is available in one field of endeavor, design incentives and other market forces can prompt variations of it, either in the same field or a different one. If a POSITA can implement a predictable variation, the invention is probably obvious. For the same reason, if a technique has

been used to improve one device, and a POSITA would recognize that the technique would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond the POSITA's skill. It is my understanding, in other words, that a court has to determine whether the improvement is more than the predictable use of prior-art elements according to their established functions. Counsel has told me that that this standard is typical and it is not confined to any particular formalistic conception.

45. Counsel has also told me that an obviousness analysis should consider the scope and content of the prior art, differences between the prior art and the claims of the challenged patent claims, and the level of ordinary skill in the art. Secondary considerations of obviousness or non-obviousness, where supplied, must also be considered. Secondary considerations can include commercial success enjoyed by devices practicing the patented invention, industry praise for the patented invention, copying by others, and the existence of a long-felt but unsatisfied need for the invention. I am also informed by Counsel that there must be a nexus between these factors and the claims themselves for these secondary considerations to have an impact on the analysis of obviousness.

46. Counsel has told me that there generally must be a motivation to combine the references in order to find obviousness. This motivation or reason to

combine can arise from the references themselves, changing market dynamics, or from simple common sense.

47. I am further informed by Counsel that a single reference can render a patent claim obvious, even if that reference does not explicitly or inherently disclose every element of the claim.

48. To determine whether there was an apparent reason to combine the known elements in the way a patent claims, it will often be necessary to look to interrelated teachings of multiple patents; to the effects of demands known to the design community or present in the marketplace; and to a POSITA's background knowledge.

IV. TECHNOLOGY BACKGROUND

49. In this section I offer some background on malware and malware-detection software, for the purpose of contextualizing my opinions on the validity of the claims of the '243 Patent. All of the concepts discussed in this section were well-known and widely used well prior to the April 2006 priority date I have assumed applies to the '243 Patent.

A. Overview of Malware

50. Malware, or malicious software, is software that targets information or other resources on a computer or network in order to modify, steal, or destroy the

data or otherwise misuse the resources. EX-1006, 1:6-22. Malware enters a computer system or network and acts on it in harmful ways. Malware may come in the form of a "virus" that inserts its own code into existing programs and may destroy, encrypt, modify, or exfiltrate data and or programs; slow system resources; or log keystrokes, screenshots, and or other user actions; and to reproduce by infecting other files and spread to other computers to repeat the process. *Id.* Malware may also exist as a "worm" that can spread without attaching itself to existing files, and can delete, encrypt, or steal data or otherwise misuse resources. *Id.*; EX-1005, 2, 20.[1] Worms generally do not require user input to reproduce, and they typically spread to other computers on a network. "Trojan horses" are malware programs that appear harmless or legitimate so that an end user will unwittingly grant them access to a computer or system. EX-1001, 1:51. For example, a Trojan horse software may appear as a regular operating-system update from Microsoft, but once installed, it may damage, disrupt, steal, infect, etc., the data or programs on a computer or network.

51. Malware enters a computer system from an external source, usually the Internet or some external storage device (*e.g.*, external hard drive or flash drive).

[1] For the sake of specificity and lack of page numbering in this reference, citations to EX-1005 herein are to annotated column numbers.

EX-1005, 1-2, 9. Malware may be hidden inside software bundles or a storage device's firmware, or it may be disguised as a recognizable program.

B. Overview of Malware-Detection Software

52. Malware detection usually involves analyzing a signature of a suspect object. EX-1006, 1:23-46. A signature is a characteristic of the malware (or other object), which identifies that object with good specificity and that uses much less space than the full object itself. *Id.* The signature may be extrinsic metadata (*e.g.*, size, name, date of creation or modification, etc.), intrinsic (certain portions of the file or code, or all of it, or a pattern somewhere within the object), a digest derived mathematically by applying a function to some or all of the object and/or its metadata, or behavioral aspects such as the use of the network, attempts at infecting other computers, or patterns of use of computer resources. The purpose of a signature is to identify a particular object (*e.g.*, malware, or alternatively, legitimate software from a reputable source) with high reliability. Malware-detection-software organizations compile the signatures for known malware and store them in a database. *Id.* That way, the software can generate signatures for objects introduced into computer systems and compare the generated signatures to those in the database. If the signature is found in the database, the object is classified as malware and isolated or otherwise handled.

53. This traditional method is effective against known malware, but it has drawbacks: It relies on an up-to-date, exhaustive database. EX-1001, 1:62-2:10. Brand-new malware can compromise a computer or network before the software provider is able to update the database with the signature for the new malware. *Id.* And if the signature is not in the database, the new malware will not be detected and may "infect" the computer or network. So the reliability of this traditional method depends in large part on up-to-date databases.

C. State of the Art

54. As of April 2006, it was well known to a POSITA, and to the general public, that computers connected to the Internet were at risk of being attacked by malicious software. Malicious software can include viruses, worms, spyware, ransomware, trojan horses, and other software-based attacks.

55. By 2006, these types of attacks, and others, were well-known, and there are many anti-virus programs available on the market to detect malware intrusions, and prevent them from happening by alerting the user and removing that malware from the system. The '243 Patent itself acknowledges that software was "available to detect and remove pestware" at the time of the invention. EX-1001, 1:55-56.

V. The '243 Patent

A. Overview of the '243 Patent

56. The '243 Patent discloses a "system and method for researching an identity of a source of activity that is indicative of pestware." EX-1001 at Abstract. The method comprises "monitoring the computer for activity that is indicative of pestware." *Id.* Based on the activity, the method identifies "an object residing on the computer that is a suspected pestware object." *Id.* The method further identifies "a particular source that the suspected pestware object originated from" by "accessing at least a portion of a recorded history of sources that the computer received files from." *Id.* The source of the suspicious object is then reported. *Id.* at Fig. 4, 8:32-38.

57. The '243 Patent discloses that an "activity monitor 116 in several embodiments monitors activities on the computer and stores information about the activities in the activity log 120 so as to assist the research module 108 in identifying activities associated with pestware and the source of the pestware." *Id.* at 5:22-26. In some embodiments, the "the activity monitor 116 is realized by a kernel-mode driver that may be loaded during a boot sequence for the protected computer or anytime later. In these embodiments, the activity monitor 116 is configured to log API calls in the activity log." *Id.* at 5:42-46, Fig. 1.

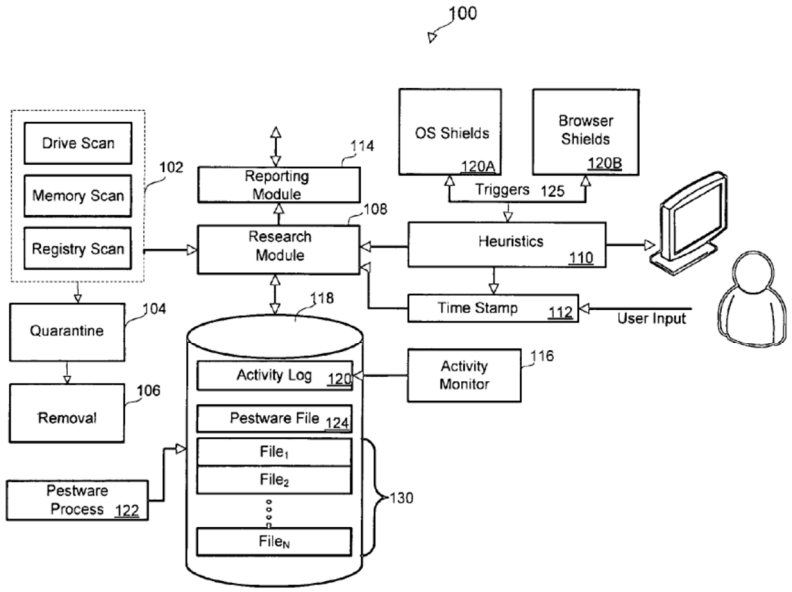

FIGURE 1

Id. at Fig. 1.

58. The activity log is stored on a file storage device, and "may include information about processes running on the computer 100 and files corresponding to the processes. In variations, the activity log 220 includes a history of API calls and respective times made by processes running on the protected computer." *Id.* at 6:12-16. The file storage device also "includes a browser history 240, browser cache 242, browser settings 244, OS settings 246, an event log 248, a debugging log 250, a firewall log 252, file information 254 and monitoring software logs 256" as depicted in Fig. 2 shown below. *Id.* at 6:17-21, Fig. 2.

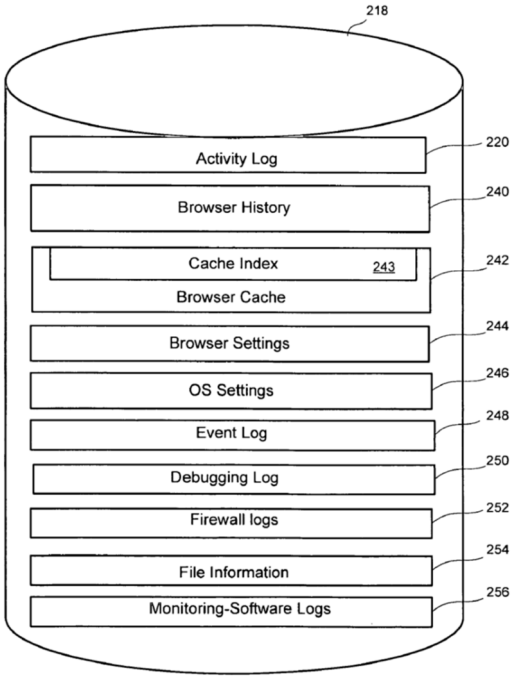

FIGURE 2

Id. at Fig. 2.

59. A "detection engine 102 scans the file storage device 118, the operating system registry and executable memory of the protected computer for indicia of pestware (*e.g.*, processes or files matching pestware definitions and/or alterations to a registry entry that are consistent with pestware)." *Id.* at 7:30-35. If pestware indicia is found, the "recorded information (*e.g.*, the activity log 120 and/or the N files 130) that may include traces of the pestware is accessed [], and traversed to search for information leading to the identification of the source of the pestware." *Id.* at 7:37-40. In order to determine the origin of the pestware, "it may be necessary to access several pieces of referential data, which may be located in one or more of the files

220-256 [including activity log and other logs] before arriving at the identity of the source of the pestware." *Id.* at 7:44-47, Fig. 2. If the source of the pestware is identified, "then the source of the pestware is reported." *Id.* at 7:61-63. The computer "may also report sources of pestware to a centralized location where the URLs may be added to a list of 'bad URLs.'" *Id.* at 7:65-67.

60. Notably, during the prosecution, applicant overcame prior art rejections by making two additions to the claims, which also appear in the Challenged Claims. First, applicant added that the "source" of the object is an "externally networked source," which the applicant argued was different from a source of an attack within the host computer. EX-1002, 3, 9-10 (August 20, 2010, Amendments and Response to Office Action) ("Porras is interested not in an externally networked source suspected of originating an attack (*e.g.*, an Internet URL or Web site from which the pestware was downloaded)."). Second, applicant added the "reporting" limitation, which requires that the externally networked source be reported to an "externally networked pestware research entity so as to enable the externally networked pestware research entity to research whether the externally networked source is a source of pestware." *Id*., 2, 8-9 (November 9, 2011, Amendments and Response to Office Action). However, the specification of the '243 Patent does not specifically mention an "externally networked" source, or an "externally networked" research

entity. However, the '243 Patent specification does mention—albeit briefly—a "research entity," but provides no specific details about its implementation. EX-1001, 8:35-38; 9:50-52.

B. Overview of the Challenged Claims

61. I am informed by counsel that Petitioners are challenging three independent claims of the '243 Patent (Claims 1, 6, and 12) and 11 dependent claims (Claims 2-5, 7-11, 13-14). I have analyzed each of these claims reproduced below.

62. For the reasons I detail below, it is my opinion that each of these claims is invalid as obvious over the prior art discussed below.

VI. PRIOR ART CONSIDERED

63. I provide below prior-art references with exemplary citations identifying the relevant features related to the claim language of the Challenged Claims. I have also described combinations of these prior-art references that, when combined, render the Challenged Claims of the '243 Patent obvious. In my opinion the Challenged Claims of the '243 Patent are rendered obvious in light of the prior art specifically discussed below.

64. The citations presented in the body of this declaration correspond to the teachings disclosed in exemplary items of prior art that identify: (1) the problem(s) confronted by one of ordinary skill in the art; (2) an express suggestion to make one

or more of the combinations; (3) an implicit suggestion to make one or more of the combinations; or (4) the knowledge of those skilled in the art as to the applicable field of technology at the relevant timeframe.

A. Identification of the Primary Prior-Art References

65. It is my opinion that a person of ordinary skill would consider at least the prior-art references below:

Prior-Art Reference	Priority Date / Date of Publication	Exhibit No.
Li, et al., *UCLog: A Unified, Correlated Logging Architecture for Intrusion Detection*¸ Int'l Conf. on Telecomm. Sys.-Modelling & Analysis (2004) ("Li")	At least by January 31, 2005	1005
U.S. Patent No. 8,117,659 to Hartrell et al. ("Hartrell")	December 28, 2005	1006
Salvador Mandujano Vergara, *A multiagent approach to outbound intrusion detection* (2004) (Ph.D. Thesis, Instituto Tecnológico y de Estudios Superires de Monterrey) ("Mandujano")	By December 9, 2004	1007
U.S. Patent No. 7,174,566 to Yadav et al. ("Yadav")	August 7, 2003	1008

66. In addition, a POSITA would have been familiar with standard problems, techniques, methods, architectures, and systems of the time. These would have included the following books and reports:

Prior-Art Reference **Priority Date / Date of Publication**	**Exhibit No.**
Jeff Crume, *Inside Internet Security: What Hackers Don't Want You to Know* (Pearson Educ. Ltd. 2000)	1011
Information Sciences Institute, Univ. of S. Cal., *Internet Protocol: DARPA Internet Program Protocol Specification* (1981)	1012
Mandia, K. & Prosise, C., *Incident Response: Investigating Computer Crime* 2001	1015

B. General Overview of the Primary Prior-Art References

67. The following sections provide a brief description of the anticipating prior-art systems that invalidate the '243 Patent. This discussion is not meant to be exhaustive, and my full element-by-element analysis is provided in more detail below (*see* VII. ANALYSIS OF THE CHALLENGED CLAIMS AGAINST THE PRIOR ART).

68. As mentioned before, it is my opinion that the references summarized below disclose the features of the Challenged Claims of the '243 Patent.

1. Li

69. Li was published at least by January 31, 2005, as part of the proceedings of the 12th International Conference on Telecommunication Systems-Modeling and Analysis (ICTSM). EX-1009 ¶¶43-44. Petitioner's counsel has informed me that, given this date, Li qualifies as prior art prior art under 35 U.S.C. § 102(b).

70. Li describes a malware detection system that works by detecting intrusions using a single, "unified logging architecture" that gathers and correlates data from heterogeneous sources. *Id*. Li explains that prior art antivirus software, such as those I described above, work primarily by using manually defined signature definitions to identify malware, which did not correlate information recorded and stored in different logging components, such as "tcpdump logs" or "system call logs." *Id.*, 2. As a solution to this issue, Li discloses a "Unified, Correlated Logging Architecture," which Li calls "UCLog," which uses recorded information from multiple sources, including a "Kernel API Logger" that logs (*i.e.*, stores a history of) kernel-level API calls, and a "Network Logger" that logs network communications. *Id.*, 9. Li also teaches analyzing the computer activity to identify abnormal activity (*i.e.*, suspected malware) based upon a heuristic (*i.e.,* rule-based) algorithm and a threshold. *Id.*, 6-7. Li further discloses that once an intrusion is detected, Li discloses tracing back through the data logged in UCLog to determine the source and execution path of the intrusion. *Id.*, 13.

2. Hartrell

71. Hartrell was filed December 28, 2005, and issued on February 14, 2012. EX-1006. Petitioner's counsel has informed me that, given this date, Hartrell qualifies as prior art prior art under 35 U.S.C. § 102(e).

72. Hartrell discloses a malware detection system that is capable of determining the source of an intrusion. *Id.*, Abstract (disclosing a "malware analysis system that helps determine, for automating cause and effect analysis of malware infections."). Hartrell explains that a problem with current malware detection systems is that "system administrators are unable to determine the root cause or origin of . . . malicious code." *Id.*, 1:23-41-42. To resolve this issue, Hartrell proposes, similar to Li, a centralized data store that receives "snapshots" of "local system and network activity" from monitored computers when malware is detected. *Id.*, 10:23-50, 3:38-53. Hartrell further discloses that the centralized data store may use information received from different computers to determine, for example, "that each of these ten computer systems visited the same web site within one minute prior to infection" and a "recommendation to block this web site." *Id.*, 10:23-50.

3. Mandujano

73. Mandujano was published by December 9, 2004. EX-1009, ¶¶39, 44. Petitioner's counsel has informed me that, given this date, Mandujano qualifies as prior art prior art under 35 U.S.C. § 102(b).

74. Mandujano discloses, in relevant part, a malware detection system that can identify potential malware on a computer system. EX-1007, 3-6. Mandujano

describes the process for identifying malware by using different weighted factors to determine a "weighted" score. EX-1007, 106-113. Mandujano further discloses that, based on the weighted score from the analysis, different actions can be taken to address the malware, depending upon whether that weighted score meets certain pre-determined thresholds. *Id.*

4. Yadav

75. Yadav was filed on February 1, 2002, and issued on February 6, 2007. EX-1008. Petitioner's counsel has informed me that, given this date, Yadav qualifies as prior art prior art under 35 U.S.C. § 102(e).

76. Yadav describes an intrusion detection system that helps determine the source of an intrusion. EX-1008, Abstract. Yadav discloses an integrated network intrusion detection that may single out specific sources of network communication (source of the intrusion) for greater scrutiny. *Id.*, Abstract, Fig. 1. For example, Yadav explains that the intrusion detection system "may use various alert levels to trigger heightened monitoring states, alerts sent to a security operation center, and/or logging of network activity for later forensic analysis. The system may monitor network traffic to block traffic that violates the network policy, monitor blocked traffic to detect an intrusion prelude, and monitor traffic from a potential intruder when an intrusion prelude is detected." *Id.*, Abstract. Yadav further explains that

information from multiple sources may be sent to a central security server, which will store information about certain network sources that will be scrutinized more heavily. For example, Yadav discloses that:

> The present inventor recognized the potential advantages of integrating firewall filtering information with network intrusion analysis. In typical network environments, most network traffic is legitimate and only a small portion of network communications may contain intrusions. By performing intrusion analysis on packets blocked by a firewall, intrusion preludes may be detected (including detection using fabricated responses to blocked network requests), and particular sources of network communications may be singled out for greater scrutiny. Thus, an overall amount of network traffic that needs to be monitored may be reduced, real-time intrusion detection may be improved, and more information about an intruder and the intruder's system and/or network may be obtained.

Id., 3:1-14, *see also id.*, 5:33-41.

VII. ANALYSIS OF THE CHALLENGED CLAIMS AGAINST THE PRIOR ART

A. Claim Construction

77. I apply the plain and ordinary meaning for the terms below, as they would have been understood by a POSITA at the priority date of the patent, as well as Patent Owner's constructions that Patent Owner has advocated for.

78. Where I address the preamble of a claim, I am not opining regarding whether the preamble imposes limitations on the claim's scope as a matter of claim construction. Instead I am opining that, to the extent the preamble is limiting, it is disclosed for the reasons I describe below.

B. Application of the Prior Art to the Claims

79. Based upon my review of the prior art, it is my opinion that the subject matter of each of the Challenged Claims would have been obvious to one of ordinary skill in the art in view of the known prior-art references.

80. I am informed by Counsel that each of the prior-art references analyzed in this declaration meets the legal requirements for prior art to the ’243 Patent. I have performed my analysis with this understanding.

81. Based upon my analysis, it is my opinion that the Challenged Claims of the ’243 Patent are rendered obvious by the following prior art:

Ground	Claims	Opinions
1	1-14	§ 103 by Li in view of Hartrell
2	1-14	§ 103 by Li in view of Hartrell and Mandujano
3	1-14	§ 103 by Li in view of Yadav
4	1-14	§ 103 by Li in view of Yadav and Mandujano

C. Ground 1: Li in View of Hartrell Renders Obvious Claims 1-14

82. In my opinion, Claims 1-14 of the ’243 Patent are obvious over Li in view of Hartrell.

1. Motivation to Combine and Reasonable Expectation of Success

83. It is my opinion that a POSITA would have been motivated to combine the teachings of Li and Hartrell. The combination of the teachings of these references would produce the obvious, beneficial, and predictable result of

implementing Li in a broad-scale system, including by allowing for the consolidation of information concerning potential threats across a network of multiple computers.

84. In my opinion, a POSITA considering the teachings of Li would have been motivated to also consider the teachings of Hartrell, as both Li and Hartrell pertain to the same field of endeavor of intrusion detection systems and methods. EX-1005, 1; EX-1006, Abstract; EX-1007, 3-6. As I discussed above, Li describes an intrusion detection system with a unified log architecture (UCLog) that logs computer activity, and can be used to trace a detected intrusion back to the source of the intrusion. EX-1005, 1, 13. Hartrell also describes an intrusion detection system that can also trace a pestware intrusion back to the source of the intrusion. EX-1006, 2:51-57. Hartrell further explains that the information gathered about a pestware intrusion and the source of the intrusion can be sent to a centralized server where it can be tracked and aggregated for different computers across a network. *Id.*, 10:36-43. As such, Li and Hartrell are in the same field of endeavor and are both analogous to the claimed invention of the '243 Patent.

85. Additionally, it is my opinion that a POSITA would have also been motivated to combine the teachings of Li and Hartrell because doing so would allow a POSITA to obtain predictable and beneficial results. As I previously explained, Li describes creating a unified log (UCLog) of computer activity, including system

and network events on a computer, and that "[d]istributed loggers are very useful and can be implemented to log system-wide information." EX-1005, 10. Additionally, Li states that "[o]btaining a system-wide view is very helpful for intrusion detection, and related malicious activities may appear in several hosts." *Id.*, 10-11. Hartrell also describes combining information from multiple logging components on multiple computers in a centralized storage location so as to make pestware determinations with information from multiple computers. EX-1006, 10:36-43. It is my opinion that a POSITA would have known to modify the teachings of Li in view of Hartrell because doing so would allow for the aggregation of the system-wide unified log of monitored computer activity collected in Li, within the centralized database described in Hartrell. A POSITA would have understood that if multiple computers were all infected with pestware after having network communications the same source, that source would more likely be a malicious source than if only one computer was infected by a source, reducing the likelihood that that source is incorrectly identified as a malicious source; in other words, a false positive.

2. Independent Claim 1

[1P]: A method for identifying an origin of activity on a computer that is indicative of pestware comprising:

86. In my opinion, to the extent that the preamble of the '243 Patent is claim-limiting, Li teaches "[a] A method for identifying an origin of activity on a computer that is indicative of pestware comprising[.]"

87. Li expressly discloses that a "key advantage" of the UCLog is "the ability to trace back and identify the source and the execution path of the occurring intrusion." EX-1005, 13. Li further explains that the disclosed UCLog "can be used to automatically identify the source and the execution path of the intrusion." *Id.*, 2. It is my opinion that a POSITA, reading these disclosures in Li, would understand that Li is disclosing a method for identifying the origin of a malicious program on a computer.

88. In my opinion, it is also clear that the disclosure in Li teaches the identification of an origin of "pestware," as that term is understood in the context of the '243 Patent, and as proposed in Petitioner's proposed construction set forth herein. Indeed, the '243 Patent explains that "[p]ersonal computers and business computers are continually under attack by trojans, spyware, and adware, collectively referred to as 'malware,' 'spyware' or 'pestware.'" EX-1001, 1:43-45. The '243 Patent goes on to state that "'pestware' as used herein refers to any of these programs that collects information about a person or an organization." *Id.*, 1:52-54. Similarly, Li discloses that the UCLog is designed to detect malware, such as viruses and

worms; specifically making reference to the "Yaha" virus, which Li discloses "reads the address book and sends itself to the contacts." EX-1005, 20. Given the '243 Patent's disclosure that "pestware" can include any program that collects information about a person or organization, it is therefore my opinion that a POSITA would have understood that the "Yaha" virus of Li would be an example and implementation of the type of pestware defined in the '243 Patent. EX-1001, 1:51-53 ("Unless specified otherwise, 'pestware' as used herein refers to any of these programs that collects information about a person or an organization.").

89. Moreover, it is my opinion that it would have been obvious to a POSITA that the intrusions described in Li would include the types of intrusions that collect information about a person or organization (*i.e.*, pestware), as disclosed in the '243 Patent. As previously discussed, malicious programs such as "spyware," which generally allow users to surreptitiously access a target computer's information, were well-known and common at the time of the publication of Li. A POSITA would understand that the intrusions contemplated in Li would include intrusions by malicious programs such as "spyware," which perform the same functions as the pestware defined in the '243 Patent.

90. Alternatively, it is my opinion that it would have been obvious to a POSITA to combine the teachings in Li with those in Hartrell, for the reasons I

explained above, such that the intrusion detection taught in Li would include the detection of malicious software designed to collect information about a person or organization. For example, Hartrell discloses that "[t]he snapshot of the activities can then be analyzed to determine the 'root cause' or source of the infection (*i.e.,* the activities that led to the infection), including, for example, how the infected computer system was discovered, how the infected computer system was accessed, what operating system objects were manipulated, and the like." EX-1006, 2:51-57. Hartrell further explicitly discloses the detection of "spyware," which is pestware as described in the '243 Patent as I explained above. *Id.*, 1:23-26, 10:22-50. Therefore, a POSITA would have considered it obvious that the UCLog intrusion detection system disclosed in Li would include the ability to identify and detect the source or origin of activity of spyware (such as pestware) on a computer, and would have been motivated to use the system for that purpose.

[1A]: monitoring, using a kernel-mode driver, the computer for activity that is indicative of pestware, wherein the monitoring includes monitoring API calls and storing a history of at least a portion of the API calls in an activity log;

91. Li discloses "monitoring, using a kernel-mode driver, the computer for activity that is indicative of pestware, wherein the monitoring includes monitoring API calls and storing a history of at least a portion of the API calls in an activity log[.]"

92. It is my opinion that Li expressly discloses the monitoring of API calls through a kernel-mode driver for activity that is indicative of pestware. Indeed, Li discloses that "[a] logger records information about the behavior of a particular part of the environment and transmits that data to the corresponding monitor." EX-1005, 9. Li further discloses that the monitors "are responsible for filtering and classifying the stream entries, and detecting any abnormal behavior." *Id.*, 11. Moreover, Li describes a "Kernel API Logger" that "should record system calls, the parameters of those calls, and the time at which they are made." *Id.*, 9. In my opinion, a POSITA would therefore have understood that the disclosed Kernel API Logger would have necessarily been proving kernel API activity to the monitor, and that API activity would then be stored in an "activity database" that "stores and manages audit data." *Id.*, 12.

93. Moreover, Li also explains that "[e]ach logging module must be coupled with the subsystem from which the logger is collecting audit data." *Id.*, 9. As such, it is my opinion that a POSITA would have understood that the most logical way to implement a kernel API activity logger would be to use a kernel-mode driver so that it could be "coupled with" the kernel API subsystem. In my opinion, a POSITA would also understand that a kernel-mode driver would be needed to obtain kernel access. I note that Li additionally discloses using loggers like WinDump and

FileMon, which a POSITA would have understood to also require using kernel-mode drivers. A POSITA would understand that without access to the kernel from a kernel-mode driver, it would not have been possible for the monitor to accurate track all of the kernel API calls. Additionally, as I discussed *supra* in [1P], Li specifically monitors a computer system for activity that is indicative of pestware and other types of intrusions.

[1B]: analyzing, heuristically, computer activity to determine whether one or more weighted factors associated with an activity exceeds a threshold so as to arrive at a determination that the activity is indicative of pestware;

94. Li discloses "analyzing, heuristically, computer activity to determine whether one or more weighted factors associated with an activity exceeds a threshold so as to arrive at a determination that the activity is indicative of pestware[.]"

95. In my opinion, a POSITA would understand that the heuristic analysis disclosed in the '243 Patent would be to use a set of rules (*i.e.*, heuristics) to determine whether computer activity would be indicative of pestware when the activity meets a "threshold for abnormality." EX-1005, 19, *see also* EX-1011 at 171 ("Many antivirus tools also perform heuristic analysis, which allows them to spot certain abnormal behaviours which can signal a viral infection."). As such, Li discloses this limitation, as Li describes "experiments . . . to justify that the correlation [between logs of different system components] can potentially increase

the accuracy of an intrusion detection system." EX-1005, 6. Li explains that in order to "train and test" the intrusion detection system, "a data-mining algorithm" is employed "to trace data to extract useful behavior patterns. The rules generated by [the data-mining algorithm] are used to classify normal and abnormal system call sequences." *Id.* Li also explains that the rules obtained from the training data are then applied to "each sequence of system calls" to predict if that sequence is "'normal' or 'abnormal' according to the rules." *Id.* "If the number of abnormal prediction [sic] in a region is greater than a half, we predict the region as 'abnormal.'" *Id.*, 6-7. As such, Li discloses analyzing using heuristics (*e.g.*, rules generated by the data-mining algorithm) of computer activity (a sequence of system calls) to determine whether one or more factors (different input) meet a threshold (more than 50%) such that the monitored activity qualifies as being indicative of an intrusion by a malicious program (*e.g.*, pestware). *Id.*, 20 ("For example, in a30, the abnormality is 48% with correlations, whereas the abnormality without correlations only gives 19%, a factor of improvement of 2.5."). As such, it is my opinion that it would have been obvious to a POSITA that using a training algorithm, these different factors disclosed in Li could have each been differently weighted, depending on the likelihood that those factors are indicative of an intrusion. As such, a POSITA would have been motivated to weigh each factor differently in the

calculation of the heuristics (rules) in order to determine whether or not an activity is accurately detecting activity indicative of an intrusion.

96. Alternatively, in my opinion it would have been obvious to a POSITA that the heuristics (*e.g.* rules) disclosed in Li could be based upon factors, such as the "abnormal increase in the network traffic," or number of "file I/O" operations disclosed in Li. EX-1005, 7, 19-20. For example, Li discloses that "[t]he information from our file I/O monitor is correlated with the other logs in the same way as we correlated the network traffic logs…. Then we reprocess the system call data taking into account any anomalies in the network traffic along with the new information from the file I/O monitor…. If the file I/O monitor detects the expected abnormal behavior, it increases the abnormality number." *Id.*, 20. It is my opinion that a POSITA would have understood that there are a number of different factors that may be indicative of a malicious intrusion, such as abnormal increases in network traffic, number of file input/output operations, and registry modifications. However, a POSITA would understand that while these factors may be indicative of an intrusion, these factors could also be the result of normal computer usage and non-malicious programs running on a computer system. As such, a POSITA would understand that some of these factors may be more indicative of an intrusion than other factors, and would also understand that the types of rules generated by a data

mining algorithm would produce "rules for system call sequences, and statistics methods for other logs." *Id.*, 14.

97. Given the foregoing, it is my opinion that it would have been obvious to a POSITA to weight different factors differently to accurately detect actual malware intrusions. Given this understanding, a POSITA would have been motivated to weigh each factor differently in calculating the likelihood that a suspicious or abnormal computer activity is indicative of an intrusion. As such, to the extent that Li does not explicitly teach using weighted factors for its disclosed rules, in my opinion, it would have been obvious to a POSITA to modify the rules in Li to have the rules be weighted, and then compare that result to the threshold disclosed in Li (*e.g.*, 48% vs. 50%).

[1C]: identifying, based on the activity, an object residing on the computer that is a suspected pestware object;

98. Li discloses "identifying, based on the activity, an object residing on the computer that is a suspected pestware object[.]"

99. As I discussed above in [1PRE] and [1A], Li discloses monitoring and collecting computer activity in the UCLog, which is then used to identify activity on the computer that is indicative of an intrusion. Moreover, as I further discussed above in [1B], Li discloses using rules (*i.e.*, heuristics) and thresholds in order to analyze whether suspected computer activity is in fact malicious. Indeed, Li

discloses identifying an object on the computer that is responsible for the intrusion as suspected malware, as Li discloses that "a key advantage of the UCLog architecture is the ability to trace back and identify the source and the execution path of the occurring intrusion," (EX-1005, 13) and also discloses that "[a]t an intrusion, UCLog can be used to automatically identify the source and the execution path of the intrusion." *Id.*, 2. As such, a POSITA reading these disclosures in Li would understand that Li teaches the identification of a suspected malicious object, as Li's disclosure of using the execution path to trace back and identify the source of the intrusion would necessarily result in the identification of the specific object on the computer that contains the suspected intrusion, such as pestware, and also the network activity that led to the transmission of that object.

100. Moreover, and alternatively, when the source and the execution path of the suspected object is determined, it would have been obvious to a POSITA to use the execution path to identify the specific object on the computer associated with that execution path, as a POSITA would consider obvious the exercise of locating the specific object on the computer associated with the suspected intrusion in the process of detecting and preventing intrusions from occurring. Indeed, the determination of the object of the source of a suspicious execution path would be one of the most logical ways to determine the source and nature of the intrusion.

Also, it would have been obvious to a POSITA to check the object name to determine if that name matched the name of any known intrusions.

[1D]: accessing, in response to the identifying an object, at least a portion of a recorded history of externally networked sources that the computer received files from so as to identify a reference to an identity of a particular externally networked source that the suspected pestware object originated from; and

101. Li discloses "accessing, in response to the identifying an object, at least a portion of a recorded history of externally networked sources that the computer received files from so as to identify a reference to an identity of a particular externally networked source that the suspected pestware object originated from[.]"

102. Li discloses that, upon detecting a suspected intrusion (such as pestware), Li discloses tracing back through UCLog to "identify the source and execution path of the occurring intrusion." EX-1005, 13; *id.*, 2 ("At an intrusion, UCLog can be used to automatically identify the source and the execution path of the intrusion."). Based on this disclosure, a POSITA would also understand that the "source" of Li would have included an externally networked source, because the execution path of the intrusion would already identify the source object on the computer if it was received from an externally networked source. As such, a POSITA would understand the "source" in Li in that scenario to refer to an externally networked source from which the object came. Moreover, it is my opinion that a POSITA would have understood that intrusions commonly arose from external

sources, such as the Internet. A POSITA would have also understood that it would be just as likely, if not more so, for an intrusion to originate from an external source (such as the Internet), as an internal source (such as a USB drive). As such, it is my opinion that a POSITA would have understood the "source" to refer to an external source from which the object came. Alternatively, it is my opinion that a POSITA would have understood that the source refers to both the externally networked source from which the object came and the object on the computer that triggered the detection of pestware.

103. This conclusion is also supported by related teachings in Li pertaining to the computer activity collected in the UCLog, particularly in view of how common it would be for an intrusion to originate from an internally networked source. For example, Li discloses that UCLog includes a "network logger" that "record[s] all packets passing through the system, all packet headers received by the system or even higher, summary-level information." EX-1005, 9. Moreover, Li also discloses that UCLog includes a WinDump Log that "contains the contents of the UDP and TCP packet headers of all traffic to and from the client machine." *Id*., 17. A network logger and WinDump Log would both be used for monitoring activities between a computer system and an outside source, such as an externally networked source. Furthermore, Li discloses that the information recorded for

network connections includes the "sourceHost," which a POSITA would understand is the source address of the network connection: "The activity database consists of a set of tables, each corresponding to the filtered log entries from a monitor. Each table describes some measurable and distinct aspect of system behavior. For example, in our prototype implementation, there is a table … for network connections recording <startTime, duration, sourceHost, destHost, bytesFromSource, bytesFromDest, processId, etc>" *Id.*,at 6. As such, it is my opinion that a POSITA would have readily understood that these packet headers would necessarily be used for checking for intrusions originating from externally networked sources.

104. Additionally, a POSITA would understand that the packet headers disclosed as being tracked and recorded in the unified log would necessarily include the IP address of the source. *See* EX-1012, 11. The IP address would indicate which network host traffic originates from, as an IP address is the standardized way to identify a system connected to the Internet. As such, it would have been obvious to a POSITA to check the source IP address, as included in the packet headers tracked/recorded by Li, to identify the source of a potentially malicious source. Furthermore, each network connection table entry of Li includes a portion of the recorded history of data received from the external host indicated by the

"sourceHost" entry, as well as an entry for "bytesFromSource" that indicates the amount of data received from the source.

105. To the extent that Li itself does not disclose this limitation, it would have been obvious to a POSITA to modify the teachings in Li with the teachings in Hartrell, for the reasons I explained above. As in Li, Hartrell discloses "monitoring all activities that modify local data stores (*e.g.*, file system, registry, databases, etc.) and network activities (*e.g.*, TCP/IP connections, web site visits, etc.)." EX-1006, 10:25-28. Moreover, Hartrell discloses checking recorded records to identify a website (*e.g.*, an externally networked source) to determine where malware originated. For example, Hartrell discloses that "the commonality analysis process may indicate that each of four infected machines visited the same web site prior to being infected. Here, the malware analysis system may determine that this web site most likely served the malware to each of the infected machines. Using the expert system, the malware analysis system may recommend that this web site be 'blocked.'" *Id.*, 3:49-53. Hartrell also discloses that "[t]he malware analysis system performs the commonality analysis and discovers that each of these ten computer systems visited the same web site within one minute prior to the infection. The malware analysis system may alert the system operator of all ten infected computer systems to the pattern, and provide a recommendation to block this web site at their

organization's egress points to prevent future infections." *Id.*, 10:44-50. As such, Hartrell discloses reviewing recorded computer activity pertaining to a malware intrusion in order to determine the source of that malware intrusion from an externally networked source (*e.g.*, in Hartrell, a website).

[1E]: reporting the identity of the particular externally networked source to an externally networked pestware research entity so as to enable the externally networked pestware research entity to research whether the particular externally networked source is a source of pestware.

106. Li discloses "reporting the identity of the particular externally networked source to an externally networked pestware research entity so as to enable the externally networked pestware research entity to research whether the particular externally networked source is a source of pestware."

107. I take no position as to how "externally networked pestware research entity" should be construed. But it is my opinion that this limitation is disclosed in multiple ways. Li and Hartrell both disclose sending information about the source of a suspected object to an administrator, who would be on a separate computer or externally networked pestware research entity. Li states that the disclosed system can "trace back to the source and the execution path of an intrusion, relieving administrators from manually examining the logs to find such information." EX-1005, 25. Li also discloses that the user interface of an IDS "enables an administrator to view the output from the system." *Id.*, 5, 13. A POSITA would have considered

it obvious that if the administrator's user interface operates on a separate system, that system would necessarily be externally networked. Li also states that "[a]nother solution is running the activity database on a dedicated server." *Id.*, 14. Given this disclosure, it is my opinion that a POSITA would understand that, in that case, the administrator would be on an externally networked research entity to which the source was reported.

108. Like Li, Hartrell discloses that "[t]he malware analysis system may alert the system operator of all ten infected computer systems to the pattern, and provide a recommendation to block this web site at their organization's egress points to prevent future infections." EX-1006, 10:47-50. As such, it is my opinion that a POSITA would understand that, in that case, the administrator would be on an externally networked research entity to which the source was reported.

109. Additionally, Hartrell discloses logging or "monitoring all activities that modify local data stores (e.g., file system, registry, databases, etc.) and network activities (e.g., TCP/IP connections, web site visits, etc.)." *Id.*, 10:25-28. Hartrell also discloses providing a snapshot of "local system and network activity to a centralized data store." *Id.*, 10:39-40. Hartrell describes providing a snapshot that includes information such as an identified operating system object or network object involved in the monitored activity (*e.g.*, file name, socket, IP address, logical paths,

etc.); the details of the change (*e.g.*, create file, listen on network socket, etc.); if applicable, the details of the object prior to the change; the source(s) of the change (*e.g.*, process id, user security context, logical storage identity from which data originated, logical storage identity where the change occurred, network sources such as uniform resource locator (URL) or Internet protocol (IP) address, the API call used to make the change, etc.); a date and time stamp in which the event occurred. *Id.*, 4:6-16. Hartrell then discloses that the centralized data store uses the website location (URL) and IP addresses of the externally networked source to determine whether the externally networked source is a source of malware, such as pestware. For example, Hartrell discloses that "the commonality analysis process may indicate that each of four infected machines visited the same web site prior to being infected. Here, the malware analysis system may determine that this web site most likely served the malware to each of the infected machines. Using the expert system, the malware analysis system may recommend that this web site be 'blocked.'" *Id.*, 3:49-53. Hartrell further discloses that "[t]he malware analysis system performs the commonality analysis and discovers that each of these ten computer systems visited the same web site within one minute prior to the infection. The malware analysis system may alert the system operator of all ten infected computer systems to the

pattern, and provide a recommendation to block this web site at their organization's egress points to prevent future infections.". *Id.*, 10:44-50.

110. In view of these disclosures, it is my opinion that a POSITA would have understood that the disclosed centralized data store of Hartrell would be an externally networked pestware research entity that can determine whether an externally networked source is a source of pestware. Hartrell also discloses sending the externally networked source information to a centralized data store so that the system can make correlations between intrusions on different computers to determine if that source is malicious. For example, Hartrell discloses that:

> In some embodiments, the malware analysis system may perform commonality analysis on the normalized activities in the pre-infection snapshot and/or the post-infection snapshot to find any recurring activities. Once the malware analysis system discovers what the commonality is between the snapshots, the malware analysis system can tailor and provide a recommendation for responding to the detected infection. The malware analysis system can utilize an expert system to tailor and provide a recommendation based on the commonality analysis. For example, the commonality analysis process may indicate that each of four infected machines visited the same web site prior to being infected. Here, the malware analysis system may determine that this web site most likely served the malware to each of the infected machines. Using the expert system, the malware analysis system may recommend that this web site be "blocked."

Id., 3:38-53, *see also id.*, 10:23-50.

3. Dependent Claim 2

[2P]: The method of claim 1,

111. I incorporate my analysis for independent Claim 1 by reference.

[2A]: wherein the particular externally networked source is identified by an identifier selected from the group consisting of an I.P. address and a URL.

112. Li and Hartrell disclose "wherein the particular externally networked source is identified by an identifier selected from the group consisting of an I.P. address and a URL."

113. As I discussed above with respect to [1D] and [1E], the combination of Li and Hartrell disclose that the externally networked source may be identified by an IP address or a URL. I incorporate my analysis for those limitations herein by reference. For example, and as discussed, Hartrell explicitly discloses using either an IP address or a URL to identify the external source of the suspected intrusion. EX-1006, 4:3:3-16. Moreover, and as further discussed, Li discloses the use of Internet packet headers (which would inherently contain the IP address) to identify the external source of the suspected intrusion. EX-1006, 9, 17. As such, a POSITA would consider it obvious to use either an IP address and/or a URL to identify the externally networked source of the suspected intrusion.

114. Moreover, and alternatively, a POSITA would consider it obvious to use either an IP address or URL to determine the identity of the external source of

the suspected intrusion, because IP addresses and URLs are two of the most common identifiers of networked computers, and indeed most common ways to refer to networked computers.

4. Dependent Claim 3

[3P]: The method of claim 2,

115. I incorporate my analysis for Dependent Claim 2 by reference.

[3A]: wherein the identifying includes accessing an activity log that includes information that relates the activity to the suspected pestware object.

116. Li discloses "wherein the identifying includes accessing an activity log that includes information that relates the activity to the suspected pestware object."

117. As I discussed above with respect to [1A], Li discloses an activity log, which Li refers to as UCLog, that includes various information relating to computer activity. EX-1005, 9-11. Li also discloses that as the UCLog logs computer activity, the UCLog would include activity pertaining to a suspected intrusion, such as by a pestware object. *Id.* As such, it would be obvious to a POSITA reading Li to use the UCLog to identify the externally networked source of the suspected pestware, as the UCLog would include the activities of the suspected pestware object. Moreover, as discussed above in [1C] and [1D], Li discloses using the UCLog to identify anomalous behavior and to trace the log back to identify the source and execution path of the anomalous behavior. Indeed, it would be obvious to a POSITA that if

the UCLog of Li did *not* contain any information relating to the activity of the suspected pestware object, the system in Li could not have detected any anomalies in the system, as Li explains that the analysis and determination of whether a specific object is an intrusion is based on the analysis of the gathered information in UCLog.

118. In the alternative, a POSITA would have considered it obvious that UCLog would contain information about activities related to the suspected intrusion/pestware product, because the system of Li, as discussed, would not have been able to detect those suspected objects or perform, as Li discloses, the tracing back of the suspected activity back to the source intrusion.

5. Dependent Claim 4

[4P]: The method of claim 1,

119. I incorporate my analysis for Independent Claim 1 by reference.

[4A]: wherein the recorded history resides in a browser cache, which includes information about files downloaded to the computer and a source of each of the files.

120. Li discloses "wherein the recorded history resides in a browser cache, which includes information about files downloaded to the computer and a source of each of the files."

121. In the '243 Patent, it is disclosed that the "file storage device 218" includes a "browser cache 242." EX-1001, 6:17-23. The disclosed browser cache "includes files, cookies, and other objects cached in connection with use of a browser

of the protected computer." *Id.*, 6:24-35. It is my opinion that both Li and Hartrell describe using the recorded history from the file system. For example, Li discloses a "File-System Logger," that can be used to "detect changes to significant blocks." EX-1005, 10. A POSITA would understand that the File-System Logger of Li would log the recorded history stored in a browser cache, as the recorded history comprises files stored in a file system. A POSITA would further understand that the recorded history stored in the browser cache would include information pertaining to the cached files that have been downloaded to the computer, including the URL network address the cached files have been downloaded from, so that future references to these files using their URLs can be properly retrieved from the cache. *See* EX-1015 at 283 ("Both browsers record browsing history and track sites that were recently visited. They also maintain a cache that contains a certain amount of the actual files and Web pages recently viewed.")

122. Moreover, it is my opinion that it would have been obvious to log browser history using an "Application-Specific Logger," as described in Li. *Id*. Indeed, a POSITA would understand that this "Application-Specific Logger" for a browser would log information such as the files that were downloaded, and the source of those files to the browser cache. As I previously stated, a POSITA would necessarily understand that the recorded history would include information from the

browser cache, information about files downloaded to the computer and a source of each of the files. *See* EX-1015 at 283 ("Both browsers record browsing history and track sites that were recently visited. They also maintain a cache that contains a certain amount of the actual files and Web pages recently viewed.")

123. Like Li, Hartrell discloses using a "snapshot" of local system and network activity. EX-1006, 10:23-50; *id.*, 5:6-12 ("The commonality analysis component may also provide the results of its processing to the other components of the malware analysis system. In some embodiments, the commonality analysis component may call out to (*i.e.*, obtain information from) other event sources, such as, by way of example, servers, firewalls, proxies, etc., to conduct further categorization and commonality analysis."). A POSITA would understand that this snapshot would have included the browser cache, which includes information about recently downloaded files and the source of those files. Indeed, it would have been obvious to a POSITA that some of the information in the snapshot disclosed in Hartrell, such as the browser cache, could have been included in the unified log (UCLog) disclosed in Li. This is because, as previously discussed, Li discloses correlating recorded information using a single, unified log (UCLog), which Li explains is more effective in identifying intrusions. As such, a POSITA would have recognized that the browser cache of a monitored system may have relevant

information about recent network activity, and would have been motivated to include such information as part of the UCLog disclosed in Li.

6. Dependent Claim 5

[5P]: The method of claim 1,

124. I incorporate my analysis for Independent Claim 1 by reference.

[5A]: wherein the recorded history resides in at least one log selected from the group consisting of an activity log, a browser history, browser cache, browser settings, operating system settings, an event log, a debugging log, a firewall log, file information and monitoring software logs.

125. Li discloses "wherein the recorded history resides in at least one log selected from the group consisting of an activity log, a browser history, browser cache, browser settings, operating system settings, an event log, a debugging log, a firewall log, file information and monitoring software logs."

126. As I discussed above in [1D], Li discloses UCLog, which is a single, unified log containing information from at least an activity log (kernel API logger), operating system settings (systems event logger), event log (system event logger), file information (file-system logger), and monitoring software logs (application-specific logger). EX-1005, 9-10. Based on the disclosure in Li, a POSITA would have understood that the information recorded in Li would have been stored in a single log (*i.e.*, the UCLog). Moreover, a POSITA would have understood and considered obvious that the storing of the UCLog selected from at least an activity

log, operating system settings, an event log, file information, and monitoring software logs, as all of the types of logs identified in the '243 Patent, would contain and include information relevant to the detection of malware, such as pestware, on a computer system.

127. Moreover, and as I discussed above in [4B], it would have been obvious to a POSITA that Li in view of Hartrell discloses that part of the recorded history would reside in a browser cache, as the browser cache would already include network activity information relevant to the detection of an intrusion of a malware object, such as pestware.

7. Independent Claim 6

128. Claim 6 is the system version of Claim 1 and is otherwise identical in the substance disclosed. Because Li and Hartrell teach Claim 1, they therefore teach Claim 6 as well.

[6P]: A system for identifying a source of activity on a computer that is indicative of pestware including:

129. Li and Hartrell disclose "A system for identifying a source of activity on a computer that is indicative of pestware including[.]"

130. In my opinion, to the extent that the preamble of the '243 Patent is claim-limiting, Li and Hartrell teach [6P]. Both Li and Hartrell teach a system for performing the method claimed in Claim 1. For example, Li discloses

"implement[ing] the UCLog on a real system running Microsoft Outlook Express on Windows 2000." EX-1005, 3., *id.*, 5 ("[T]he data collected by a logging system can be used by an IDS to detect signs of suspicious behavior."). Moreover, Hartrell discloses "[a] malware analysis system for automating cause and effect analysis of malware infections.". EX-1006, Abstract.

[6A]: an activity monitor configured to monitor API calls and to store a history of at least a portion of the API calls in an activity log, wherein the activity monitor includes a kernel-mode driver adapted to intercept the API calls;

131. Li and Hartrell disclose "an activity monitor configured to monitor API calls and to store a history of at least a portion of the API calls in an activity log, wherein the activity monitor includes a kernel-mode driver adapted to intercept the API calls[.]"

132. It is my opinion that Li and Hartrell teach [6A] for the same reasons they teach [1A], as I discussed above. For example, and as I previously discussed, Li discloses "[a] kernel API logger should record system calls, the parameters of those calls, and the time at which they are made." EX-1005, 9. A POSITA would have understood that this discloses kernel API logger is an activity monitor that is capable of storing the history of at least a portion of the API calls of a computer system, and record that activity in the UCLog. Moreover, as with [1A], a POSITA would have considered it obvious that the kernel API logger of Li would include a

kernel-mode logger, because, as I previously discussed, a kernel-mode driver would be needed to obtain kernel access for the kernel API logger. Moreover, a POSITA would have considered it obvious to adapt the kernel-mode driver to intercept the API calls so that they can be logged, as the understood purpose of the kernel API logger is to monitor and/or log API calls to the kernel.

[6B]: a heuristics module configured to identify an activity on the computer that is indicative of pestware residing on the computer and to analyze the activity to determine whether one or more weighted factors associated with the activity exceeds a threshold; and

133. Li and Hartrell disclose "a heuristics module configured to identify an activity on the computer that is indicative of pestware residing on the computer and to analyze the activity to determine whether one or more weighted factors associated with the activity exceeds a threshold[.]"

134. It is my opinion that Li and Hartrell teach [6B] for the same reasons they teach [1B] and [1C]. As discussed with respect to [1B] and [1C], Li discloses using rules (*i.e.*, heuristics) to identify activity on a computer that is indicative of an intrusion, using both weighted factors and a threshold. It is my opinion that it would have been obvious to a POSITA that the disclosed could have been used to identify potential intrusions residing on the computer, as a POSITA would understand that these teachings could be implemented on any number of computer systems, including the specific computer system here. Moreover, it is also my opinion that a

POSITA would have understood that the component that makes predictions about whether an activity is an intrusion would be the claimed heuristics module, along with the weighted factor calculations and thresholds, as disclosed in Mandujano. A POSITA would have understood that the disclosed components could be implemented in a single heuristics module, as these implementations are all parts, or steps, in the process of determining whether activity amounts to an intrusion. For example, a POSITA would have understood that a "module" is just a generic reference to a part of a system that performs a specific task and can be named anything. A POSITA would have known that it was common to name a module after the task that it performs, so "heuristics module" would have been a natural name for a part of the system that performs heuristics.

[6C]: a research portion configured to access, in response to a prompt from a heuristics module, a first set of recorded information on the computer that relates the activity to at least one file residing on the computer, and wherein the research portion is configured to access a second set of recorded information on the computer that relates the at least one file to an externally networked source from which the file was received; and

135. Li and Hartrell disclose "a research portion configured to access, in response to a prompt from a heuristics module, a first set of recorded information on the computer that relates the activity to at least one file residing on the computer, and wherein the research portion is configured to access a second set of recorded

information on the computer that relates the at least one file to an externally networked source from which the file was received[.]"

136. It is my opinion that Li and Hartrell teach [6C] for the same reasons they teach [1D]. As I discussed with respect to [1D], Li discloses tracing back through the UCLog to "identify the source and execution path of the occurring intrusion." EX-1005, 13. A POSITA would have understood that the portion of the disclosed system in Li that performed the function of tracking back through the UCLog to identify a source of an intrusion would be the research portion that performs the requirements in [6C]. Moreover, it would have also been obvious to a POSITA that the portion of the code dedicated to the tracing back through the UCLog to be a separate research portion.

137. Moreover, it is also my opinion that it would have been obvious to a POSITA that the tracing back function disclosed in Li would be performed in response to a prompt from the heuristic module described in [6B]. This is because the purpose of the heuristics module is to identify a suspected intrusion, and this tracing back would necessarily be performed when the heuristics module makes such an identification. As such, it is my opinion that a POSITA would have considered it obvious that the research portion would check for the source of an intrusion in response to a prompt from the heuristics module that identified a suspected intrusion.

Further, the information recorded in UCLog would necessarily include information on the computer. Li describes distributed loggers and loggers operating on the same computer, and so the location of access would be a design choice.

138. As I previously discussed, Li discloses UCLog, which combines multiple different sets of recorded information, including the Kernel API Logger, File-System Logger, and the Network Logger. EX-1005, 9-10. Li explains that the UCLog is traced to determine the activity of the intrusion, such as in the Kernel API Logger and File-System Logger sets (first set of recorded information). Li further describes tracing back to the source of the intrusion. *Id*. It is my opinion that it would have been obvious to a POSITA that this would have involved looking at information in a second set of recorded information, such as the disclosed Network Logger. For example, the Network Logger includes the source information the recorded packet headers., and would relate a file to the externally networked source from which that file was received. Moreover, it would be obvious to a POSITA that the recorded information in UCLog would include information that is on the monitored computer. This conclusion is supported by the disclosures in Li, as Li describes distributed loggers and loggers operating on the same computer, and so the location of access would inherently be a design choice.

139. Moreover, to the extent that [6C] would not have been considered obvious in view of Li alone, it is my opinion that it would have been obvious to combine Li with Hartrell for the reasons explained in [1D]. Indeed, Hartrell discloses a categorization component that makes a determination whether a file is malware, such as pestware, and then determines additional information about that file, including the externally networked source of that file. EX-1006, 6:66-7:15, 8:10-9:28, Figs. 3, 5, 6. It is my opinion that a POSITA would have understood that the portion of the categorization component of Hartrell that determines this additional information about a malicious file, such as the externally networked source of the file, would necessarily be the research portion that performs the other requirements of [5C]. In my opinion, at a minimum, it would have been obvious to a POSITA that the portion of the categorization component that determines additional information about a malicious file could have been a separate research portion.

140. Moreover, as I discussed *supra* in [1D], it is also my opinion that a POSITA would have considered it obvious that a determination of additional information of an intrusion would occur in response to a prompt from a portion of the categorization component that determines if a file is suspected malware, because the additional information would only need to be determined in response to a

determination that a file is malware. This is depicted in Figure 2 of Hartrell, which I have reproduced below:

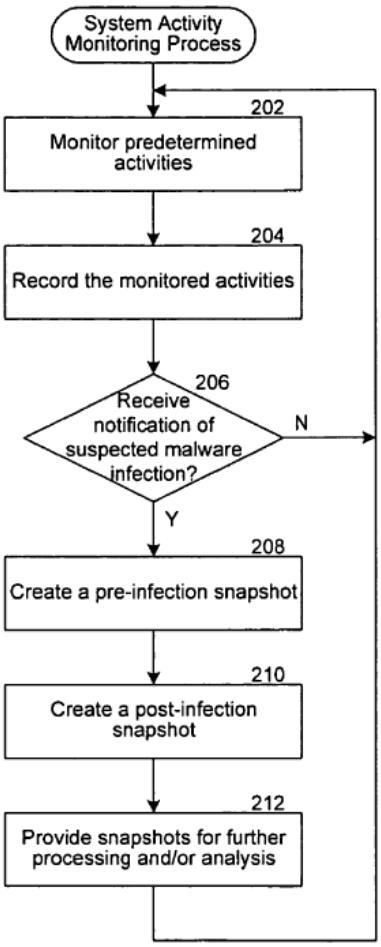

FIG. 2

Id., Fig. 2. Hartrell further explains with reference to Figure 2 that once a notification of suspected malware is received 206, it will then generate a post infection snapshot 210 that is then sent for further process and analysis 212. *Id.*, 6:32-52. As such, a POSITA would have considered it obvious that the research portion would check for the source of an intrusion in response to a prompt from

another portion—the categorization component—that identified whether or not a file is potentially malware.

141. Additionally, according to Hartrell, the categorization component receives a snapshot with a "predetermined set of common categories of system or network events." EX-1006, 7:4-5. Given this disclosure, it would have been obvious to a POSITA that the set of system events (i.e., the first set of recorded information) would be accessed by the categorization component to determine whether or not the file is behaving as malware, and categorize it appropriately. It is also my opinion that it would have been obvious to a POSITA that, when additional information about suspected malware is being determined, that the categorization component of Hartrell would access a second set of recorded information (i.e., the "network events), which would have additional information, such as the identity of the externally networked source.

[6D]: a reporting portion configured to generate a report that identifies the externally networked source of the file and to report an identity of the externally networked source to an externally networked pestware research entity so as to enable the externally networked pestware research entity to research whether the externally networked source is a source of pestware.

142. Li and Hartrell disclose "a reporting portion configured to generate a report that identifies the externally networked source of the file and to report an identity of the externally networked source to an externally networked pestware

research entity so as to enable the externally networked pestware research entity to research whether the externally networked source is a source of pestware."

143. It is my opinion that Li and Hartrell teach [6D] for the same reasons they teach [1E], as I discussed above. Additionally, Hartrell discloses, for example, generating a "snapshot of the last five minutes and subsequent five minutes of local system and network activity to a centralized data store." EX-1006, 10:38-40. A POSITA would understand and recognize that the disclosed "snapshot" would constitute the generated report that identifies the externally networked source of the file. Indeed, that report (*i.e.*, snapshot) is sent the centralized data store (*i.e.*, the externally networked pestware research entity), which then compares the snapshot against reports sent from other computers to determine whether the identified networked source is a source of malware, such as pestware. For example, and as previously identified, Hartrell explains that "[t]he malware analysis system performs the commonality analysis and discovers that each of these ten computer systems visited the same web site within one minute prior to the infection. The malware analysis system may alert the system operator of all ten infected computer systems to the pattern, and provide a recommendation to block this web site at their organization's egress points to prevent future infections.". *Id.*, 10:44-50. As such, a POSITA would have considered it obvious that the portion that generates this report,

or snapshot, for the centralized data store could be a separated reporting portion in the code. As such, it is my opinion that Li in combination with Hartrell renders this limitation obvious.

8. Dependent Claim 7

[7P]: The system of claim 6,

144. I incorporate my analysis for Independent Claim 6 by reference.

[7A]: wherein activity monitor is configured to store an identity of each process that made each of the API calls in the stored history, and wherein the activity monitor is configured to store an identity of each file that corresponds to each the processes that made the API calls in the stored history so as to create a relation between each API call and at least one file.

145. Li and Hartrell disclose "wherein activity monitor is configured to store an identity of each process that made each of the API calls in the stored history, and wherein the activity monitor is configured to store an identity of each file that corresponds to each the processes that made the API calls in the stored history so as to create a relation between each API call and at least one file."

146. Li and Hartrell teach [7A] for the same reasons that they teach [6A]. Specifically, Li discloses "[a] kernel API logger should record system calls, the parameters of those calls, and the time at which they are made." EX-1005, 9. A POSITA reading Li would understand that these API call parameters from the disclosed kernel API logger would necessarily have to include at least an identity of the process that made the API call and also the file that corresponds to the process

that made the API call. This is because the purpose of API calls is to allow one application to request data or access services from another application or from the system. The API call, or API request, thus would need to include information such as the identity of the requesting process so that data can be returned to the correct entity. Without this information from the API call, it would not be possible for the API call to submit the request to the other application and receive the correct response.

147. Moreover, Li itself further discloses tracing the API call back to the source and execution path of the intrusion. *Id.*, 13. It would have been obvious to a POSITA that in order to perform this function, the disclosed UCLog of Li would need to store the identity of the process that created the API call, and the file that created that process. Without this information, it would not be possible to trace the API call back to the source and execution path of the intrusion.

148. Alternatively, and regardless of the disclosures in Li, it would have been obvious, in my opinion, to log the API call process identity and the file that made the process. The logging of such information at the time of the API call would permit a user tracing the API call back to the source to more easily access this information, without the need to independently collect this information for each API call being investigated.

9. Dependent Claim 8

[8P]: The system of claim 6,

149. I incorporate my analysis for Independent Claim 6 by reference.

[8A]: wherein the heuristics module is configured to receive information about the API calls from the activity monitor and determine whether the API calls are indicative of pestware.

150. Li and Hartrell disclose "wherein the heuristics module is configured to receive information about the API calls from the activity monitor and determine whether the API calls are indicative of pestware."

151. Li and Hartrell teach [8A] for the same reasons that they teach [6B]. As discussed above with respect to [6B], Li discloses using rules (what the '243 Patent refers to as "heuristics") to identity suspicious activity, based on weighted factors and a threshold. Li discloses that these rules are used to determine whether API calls are "'normal' or 'abnormal' according to the rules," and where behavior that is considered "abnormal" is indicative of an intrusion by a malicious program, such as pestware. EX-1005, 6-7.

152. Therefore, it would have been obvious to a POSITA that the "heuristics module" that is inherently disclosed in Li would have access to the recorded computer activity stored in the UCLog, which as Li discloses, contains a log of API calls. *Id*. A POSITA would understand from reading Li that the disclosed heuristics module would need to have access to the information contained in the UCLog,

because without that recorded information, the disclosed heuristics module would not be able to analyze whether computer activity was normal or abnormal, undercutting the purpose of the UCLog in Li: to detect potential intrusions by malicious code, such as pestware.

10. Dependent Claim 9

[9P]: The system of claim 6,

153. I incorporate my analysis for Independent Claim 6 by reference.

[9A]: wherein the first set of recorded information and the second set of recorded information reside in the same log file on a file storage device of the computer.

154. Li discloses "wherein the first set of recorded information and the second set of recorded information reside in the same log file on a file storage device of the computer."

155. As I discussed above with respect to [1A] and [6C], Li discloses a single, unified log (UCLog) that contains multiple sets of recorded computer activity. EX-1005, 9-10. Indeed, Li discloses that the UCLog contains at least a Kernel API Logger, File-System Logger, and a Network Logger. *Id.* A POSITA reading the disclosure in Li would understand that the sets of recorded information both reside in the same UCLog file as in [6C].

11. Dependent Claim 10

[10P]: The system of claim 6,

156. I incorporate my analysis for Independent Claim 6 by reference.

[10A]: wherein the externally networked source is identified by an identifier from the group consisting of an I.P. address and a URL.

157. It is my opinion that Li and Hartrell teach [10A] for the same reasons that they teach [2A].

12. Dependent Claim 11

[11P]: The system of claim 6,

158. I incorporate my analysis for Independent Claim 6 by reference.

[11A]: wherein the recorded history resides in at least one log selected from the group consisting of an activity log, a browser history, browser cache, browser settings, operating system settings, an event log, a debugging log, a firewall log, file information and monitoring software logs.

159. It is my opinion that Li and Hartrell teach [11A] for the same reasons that they teach [5A].

13. Independent Claim 12

160. Claim 12 is the processor-executable instruction version of Claim 1 and is otherwise identical in substance. Because Li in view of Hartrell teach Claim 1, they therefore teach Claim 12 as well.

[12P]: A non-transitory computer-readable medium including processor-executable instructions for identifying an origin of activity on a computer that is indicative of pestware, the instructions including instructions for:

161. Because [12P] is the processor-executable instruction version of [1P], [12P] is invalid over the prior art for the same reasons that [1P] is invalid over the prior art.

162. Moreover, both Li and Hartrell disclose implementing the process recited in [1P] using a non-transitory computer-readable medium. For example, Li explains that the UCLog was implemented in software. EX-1005, 3 ("We have implemented the UCLog architecture on a real system running Microsoft Outlook Express on Windows 2000."). *See* EX-1006, Abstract (same).

[12A]: monitoring, with a kernel-mode driver, the computer for activity that is indicative of pestware, wherein the instructions for monitoring include instructions for monitoring API calls and storing a history of at least a portion of the API calls in an activity log;

163. Because [12A] is the processor-executable instruction version of [1A], [12A] is invalid over the prior art for the same reasons that [1A] is invalid over the prior art.

[12B]: analyzing, heuristically, computer activity to determine whether one or more weighted factors associated with an activity exceeds a threshold so as to arrive at a determination that the activity is indicative of pestware;

164. Because [12B] is the processor-executable instruction version of [1B], [12B] is invalid over the prior art for the same reasons that [1B] is invalid over the prior art.

[12C]: identifying, based upon the activity, an object residing on the computer that is a suspected pestware object;

165. Because [12C] is the processor-executable instruction version of [1C], [12C] is invalid over the prior art for the same reasons that [1C] is invalid over the prior art.

[12D]: accessing, in response to identifying an object, at least a portion of a recorded history of externally networked sources that the computer received files from so as to identify a reference to an identity of a particular externally networked source that the suspected pestware object originated from; and

166. Because [12D] is the processor-executable instruction version of [1D], [12D] is invalid over the prior art for the same reasons that [1D] is invalid over the prior art.

[12E]: reporting the identity of the particular externally networked source to an externally networked pestware research entity so as to enable the externally networked pestware research entity to research whether the particular externally networked source is a source of pestware.

167. Because [12E] is the processor-executable instruction version of [1E], [12E] is invalid over the prior art for the same reasons that [1E] is invalid over the prior art.

14. Dependent Claim 13

[13P]: The non-transitory computer-readable medium of claim 12,

168. I incorporate my analysis for Independent Claim 12 by reference.

[13A]: wherein the particular externally networked source is identified by an identifier selected from the group consisting of an I.P. address and a URL.

169. Li and Hartrell teach [13A] for the same reasons that they teach [2A].

15. Dependent Claim 14

[14P]: The non-transitory computer-readable medium of claim 12,

170. I incorporate my analysis for Independent Claim 12 by reference.

[14A]: wherein the recorded history resides in at least one log selected from the group consisting of an activity log, a browser history, browser cache, browser settings, operating system settings, an event log, a debugging log, a firewall log, file information and monitoring software logs.

171. Li and Hartrell teach [14A] for the same reasons that they teach [5A].

D. Ground 2: Li in View of Hartrell and Mandujano Renders Obvious Claims 1-14

172. In my opinion, while Li and Hartrell render obvious every limitation of Claims 1-14 of the ’243 Patent, the claims of the ’243 Patent would also have been obvious over Li, Hartrell, and Mandujano.

173. Mandujano was published by December 9, 2004. EX-1009 ¶¶ 39, 44. As such, I understand that Mandujano qualifies as prior art under 35 U.S.C. § 102(b). Mandujano discloses, in relevant part, a process for identifying suspected intrusions of malicious software onto a computer system using a process of different weighted factors to help determine a weighted “score” associated with the suspected intrusion, and then taking different actions if the calculated score meets specific thresholds. EX-1007, 106-113. A POSITA would understand that these equations that calculate

the weighted scores are the heuristics (rules) that are used to help identify potential intrusions.

1. Motivation to Combine and Reasonable Expectation of Success

174. In my opinion, a POSITA would have been motivated to combine the teachings of Li and Hartrell with those in Mandujano for multiple reasons, as I discuss in greater detail below. However, and most obviously, a POSITA would have been motivated to combine all three teachings to produce the obvious, beneficial, and predictable result of using a different scoring system to determine abnormal or potentially malicious behavior.

175. More specifically, a POSITA would have been motivated to combine the teachings of Li and Hartrell with the teachings of Mandujano because all three references pertain to the same field of endeavor: malware detection and prevention. As I discussed above, Li describes malware detection system with a unified log to track intrusions back to their source. EX-1005, 13. Similar to the teachings in Li, Hartrell too discloses a malware detection system that is capable of tracing back the detected malware to the source of the intrusion. EX-1006, 2:51-57 ("The snapshot of the activities can then be analyzed to determine the 'root cause' or source of the infection . . . including, for example how the infected computer system was accessed, what operating system objects were manipulated, and the like."). Hartrell further

discloses that once the source of an intrusion is determined, the system may relay to a centralized server this information so that it can be researched, tracked, and aggregated for use by other computers across a network. *Id.*, 10:22-50. Like Li and Hartrell, Mandujano also describes an intrusion detection system that is capable of identifying potential intrusions based on computer activity. Mandujano further discloses that potential intrusions are identified using a scoring method using various weighted factors in order to determine whether a specific object or activity is indicative of an intrusion. EX-1007, 106. Therefore, it is my opinion that Li, Hartrell, and Mandujano are in the same field of endeavor and are analogous to the claimed invention of the ’243 Patent.

176. Additionally, it is my opinion that a POSITA would have been motivated to combine the teachings of Li, Hartrell, and Mandujano, as the combination of these teachings would allow a POSITA to obtain predictable and beneficial results. As I explained above, Li describes creating a unified log of system events on a computer. EX-1005. Hartrell describes combining information from multiple computers in a centralized store so as to make malware determinations with information from multiple computers. EX-1006. Mandujano provides details of a scoring system whereby intrusions can be identified and specific action can be taken based upon whether the scores meets different thresholds. EX-1007, 106-114.

Given the foregoing, it is my opinion that a POSITA would have known to modify the teachings in Li and Hartrell based on the disclosures in Mandujano because doing so would allow for a way to score or rank potential intrusions based on the seriousness of the threat. Having threats ranked thus would allow different threats of varying levels of seriousness to be handled differently, and in the most appropriate way for that particular threat.

177. Moreover, a POSITA would have considered obvious the fact that all potential intrusions do not include the same level of risk, or threat level, to a computer system. Indeed, the potential risk and damage caused by malicious code may range from the trivial to massive data breaches, ransomware attacks, and destruction of hardware components. Therefore, a POSITA would have been motivated to provide a score that could identify the potential risk associated with an intrusion and take different actions commensurate with the score (*i.e.*, the level of risk of the particular object). As such, it would have been obvious to a POSITA to take only the level of action necessary to stop the intrusion. A POSITA would realize the benefit of not having to take what would otherwise be drastic actions to prevent an intrusion with a low threat risk from remaining on a system, as that action may result in expunging certain data and affect the performance of the system. As such, a POSITA would have therefore been motivated to try the scoring system from

Mandujano to provide different potential responses to the detected intrusion based upon the risk.

178. I note that while the disclosure in Mandujano focusses on monitoring local activity and outbound traffic (EX-1007, 3), it still discloses a malware detection system like Li and Hartrell. That Mandujano focusses on outbound monitoring is inconsequential for what Mandujano teaches, as nearly identical methods are used to monitor inbound and outbound traffic for purposes of detecting intrusions. Moreover, a POSITA would have recognized that the specific weighted factor calculations and threshold comparisons could be used in the Li-Hartrell system described above. Indeed, a POSITA would have understood that there are various ways to implement the rules-based calculations disclosed in Li, and would have been motivated to implement the rules-based system in Li through different ways, including through the system disclosed in Mandujano, to determine what specific system was the best for detecting intrusions. A POSITA would have recognized that the similarity-based equations described in Mandujano could have been used in Li, because Li also discloses comparing detected behavior with training data to determine how "normal" or "abnormal" (*i.e.*, similar or dissimilar) the detected behavior is. EX-1005, 6-7.

179. For the foregoing reasons, therefore, in my opinion, it would have been obvious for a POSITA to try to combine the Li-Hartrell system described above with the scoring system described in Mandujano to provide flexibility of responses based upon the potential threat.

2. Li over Hartrell and Mandujano Render Obvious Limitations [1B] and [1C].

180. It is my opinion that to the extent Li and Hartrell do not render obvious limitations [1B] and [1C], Li, Hartrell, and Mandujano disclose these limitations. Mandujano discloses using a "score-based system" to determine whether an object is malware. EX-1007, 106. For example, Mandujano discloses that "[a]n overall score *sigma* represents the similarity between the input packets and a determined signature. This score is composed of a linear combination of sub-scores $sigma_i$ that correspond to a match between the *i*-th attribute of the signature and the input." *Id.* Mandujano goes on to explain the specific equation that determines a weight, w_i, for each attribute based on its similarity and the weights are then combined and normalized into the range between 0 and 1 in a weighted value called σ:

$$\omega_i = ln(k) - ln(i) \quad \ldots (7)$$

$$\sigma = \sum_{i=1}^{k} \frac{\sigma_i \omega_i}{\sum_{j=1}^{k} \omega_i} \quad \ldots (8)$$

EX-1007, 106.

181. Mandujano also discloses using the weights, w_i, to calculate another score, π, which again is normalized into the range between 0 and 1:

$$\pi = \sum_{i=1}^{k} \pi_i \omega_i \qquad \ldots (10)$$

Id., 110. Mandujano discloses combining those two factors, σ and π, into an integrated score called I:

$$\begin{aligned}
&(1)\ If\ \{\exists\, H_1\ \wedge\ \nexists\, H_2\} \Rightarrow \{H_3 = H_1 \wedge I = \sigma\}\\
&(2)\ If\ \{\nexists\, H_1\ \wedge\ \exists\, H_2\} \Rightarrow \{H_3 = H_2 \wedge I = \pi\}\\
&(3)\ If\ \{\nexists\, H_1\ \wedge\ \nexists\, H_2\} \Rightarrow \{H_3 = I = NULL\}\\
&(4)\ If\ \{\exists\, H_1, H_2 \mid H_1 = H_2\} \Rightarrow \{H_3 = H_1 = H_2 \wedge I = \tfrac{\sigma+\pi}{2}\}\\
&(5)\ If\ \{\exists\, H_1, H_2 \mid H_1 \neq H_2\} \Rightarrow \begin{cases} \sigma > \pi & \Rightarrow\ H_3 = H_1 \wedge I = \sigma \\ \pi > \sigma & \Rightarrow\ H_3 = H_2 \wedge I = \pi \\ \sigma = \pi & \Rightarrow\ H_3 = I = NULL \end{cases}
\end{aligned}$$

Id., 112.

182. Mandujano also discloses that all of those weighted factors are compared against thresholds to determine what action will be taken:

Response types

```
A = send matching data to evidence repository
B = move executable to evidence repository
C = copy command history to evidence repository
D = suspend process
E = change file execution privileges
F = send kill signal to process
G = start tracing
H = alert target system
```

Traffic Monitoring Cell			
	$\sigma \geq 0.5$	$\Rightarrow$	A
	$\sigma \geq 0.7$	$\Rightarrow$	B
	$\sigma \geq 0.8$	$\Rightarrow$	C
Process Monitoring Cell			
	$\pi \geq 0.5$	$\Rightarrow$	A
	$\pi \geq 0.7$	$\Rightarrow$	B
	$\pi \geq 0.8$	$\Rightarrow$	C
Correlation Cell			
	$\sigma \geq 0.5,\ \pi \geq 0.5,\ I \geq 0.7$	$\Rightarrow$	D
	$\sigma \geq 0.5,\ \pi \geq 0.5,\ I \geq 0.8$	$\Rightarrow$	E + G
	$\sigma \geq 0.5,\ \pi \geq 0.5,\ I \geq 0.9$	$\Rightarrow$	F + H

Table 5.6: Rules to implement automated response.

Id., 114. Based on this, for example, if σ meets the threshold of 0.5, π meets the threshold of 0.5, and I meets the threshold of 0.9, the system will send a kill signal to the process (Response F) and alert the target system (Response H). Mandujano also explains that in certain applications, a single weighted factor may be used. For example, Mandujano explains "that a single score can trigger more than one reaction." *Id.*, 114.

183. It is my opinion that it would have been obvious for a POSITA to use the similarity weighted factors disclosed in Mandujano (σ, π, and I) in the rules set forth in Li. As previously discussed, a POSITA would have understood that there are a number of different factors that can be used to determine whether a malicious

program is executing on a computer. This can include changes in the number of file I/Os, registry modification, and abnormal increases in network traffic. It would be obvious to a POSITA that not all of the factors that can be used would be weighted equally, as factors that may be used to determine if malicious code is executing on a computer may also be the result of benign and user-directed non-malicious activity. As such, a POSITA, in implementing such a system, would have been motivated to determine how to appropriately weight all of the factors in an equation, such as by using the weighted factors disclosed in Mandujano. Given the foregoing, it would have been obvious to a POSITA to combine Li and Hartrell with Mandujano for the reasons I previously explained.

184. Additionally, with respect to [1C], it would have been obvious to a POSITA to use weighted factors and thresholds, such as those disclosed in Mandujano, to assist in the identification of suspected malware (such as pestware) activity as discussed above, as Li then discloses tracing back the UCLog to identify the suspected pestware object. For example, as previously discussed, Li discloses "[a]t an intrusion, UCLog can be used to automatically identify the source and the execution path of an intrusion[.]" EX-1005, 2.; *id.*, 13 (disclosing that the UCLog of Li "can trace back to the source and the execution path of an intrusion, relieving administrators from manually examining the logs to find such information.").

185. Therefore, it is my opinion that Claim 1 and its dependent limitations are rendered obvious in view of Li, Hartrell, and Mandujano.

3. Li over Hartrell and Mandujano Render Obvious Limitation [6B]

186. It is my opinion that, to the extent that Li and Hartrell do not render obvious this limitation, Li, Hartrell, and Mandujano trach [6B] for the same reasons that they teach [1B] and [1C]. Li, Hartrell, and Mandujano all disclose using heuristics (*i.e.*, rules) to identify activity on a computer that is indicative of an intrusion, based upon weighted factors and a predetermined threshold. A POSITA would have considered it obvious that these teachings could be used to identify potential intrusions residing on *the computer*, as a POSITA would understand that these teachings could be implemented on any number of computer systems, including the specific computer system here. Moreover, it is also my opinion that a POSITA would have understood that the component that makes predictions about whether an activity is an intrusion would be the claimed heuristics module, along with the weighted factor calculations and thresholds, as disclosed in Mandujano. A POSITA would have understood that the disclosed components could be implemented in a single heuristics module, as these implementations are all parts, or steps, in the process of determining whether activity amounts to an intrusion. In any event, a POSITA would have found it obvious to implement the predictions (along

with the disclosed calculations from Mandujano) based on rules (*i.e.*, heuristics) and thresholds in a separate module, which could collectively be referred to as the heuristics module, as these implementations are all parts, or steps, in the process of determining whether activity amounts to an intrusion.

187. As such, it is my opinion that Claim 6, along with its dependent limitations, are rendered obvious in view of Li, Hartrell, and Mandujano.

4. Li over Hartrell and Mandujano Render Obvious Limitations [12B] and [12C].

188. Li, Hartrell, and Mandujano teach [12B] and [12C] for the same reasons as they teach [1B] and [1C]. As such, it is my opinion that Claim 12 and its limitations are rendered obvious by Li, Hartrell, and Mandujano.

E. Ground 3: Claims 1-14 are obvious under §103 over Li and Yadav.

189. It is also my opinion that to the extent the foregoing Grounds do not render obvious the Challenged Claims, Li in view of Yadav renders obvious Claims 1-14. I understand from counsel that Yadav was published on August 7, 2003, and is therefore prior art under §102(b). EX-1008. I understand as such that Yadav can be used in lieu of Hartrell.

190. As I previously explained *supra*, Yadav, like Hartrell, discloses an intrusion detection system that assists in the determination of the source of an

intrusion. *Id*., Abstract. Yadav explains that the integrated network intrusion detection may single out specific sources of network communication (source of the intrusion) for greater scrutiny. *Id*., Abstract, Fig. 1. Yadav further explains that information from multiple sources may be sent to a central security server, which may store information about certain network sources for scrutiny and forensic analysis. *Id*., 3:1-14, 5:33-41.

1. Motivation to Combine and Reasonable Expectation of Success

191. It is my opinion that a POSITA would have been motivated to combine the teachings of Li and Yadav for a number of reasons, including to produce the obvious, beneficial, and predictable result of implementing Li on a broad scale. More specifically, a POSITA would have motivated to combine Li with Yadav as the consolidation of potential threat information from multiple computers in a network would allow for greater accuracy in the identification and detection of potential threats and the sources of them.

192. It is also my opinion that a POSITA would have been motivated to combine Li with Yadav because both references pertain to the same field of endeavor: the detection and prevention of intrusions. As I have explained, Li discloses UCLog, which is a single, unified activity log that can trace the path of a detected intrusion back to the intrusion's source. EX-1005, 13. Similarly, Yadav

discloses a malware detection system, that is also capable of tracing back detected malware to its source. For example, Yadav explains that "If an intrusion prelude is detected, the source of the intrusion prelude is identified (530). The identified source is a potential intruder, and thus communications from the potential intruder are monitored in an active monitoring state 535." EX-1008, 8:49-53. Yadav also discloses that this determined source information of an intrusion may be sent to a centralized security server where it can be tracked and aggregated along with information received from other networked computers. *Id*., 3:1-14, 5:33-41, 6:6-8. I note that while Yadav also explains that the functionalities of this disclosed method is part of a firewall, Yadav discloses that these functionalities may be integrated into monitored nodes, as Li discloses. *Id.*, 3:15-21 ("In addition, firewall functionality may be integrated with intrusion detection on end nodes (*e.g.*, servers and hosts) in a network, such as an enterprise network, to further improve intrusion detection and network security. For example, a networked machine may include an intrusion detection system that functions in part as a dynamic firewall for the networked machine."). For the foregoing reasons, it is therefore my opinion that Li and Yadav are in the same field of endeavor, and are analogous to what is claimed as the invention in the '243 Patent.

193. A POSITA, in my opinion, would have also been motivated to combine Li with Yadav because the combination of the teachings of both references would yield predictable and beneficial results. As I have explained *supra*, Li describes creating a unified log of system events on a computer. EX-1005, 1. Similar to Li, Yadav describes combining information about intrusions from multiple computers to make malware determinations. *Id*., 3:1-14, 5:33-41, 6:6-8. A POSITA, reading both Li and Yadav, would be motivated to modify the disclosure in Li in view of the disclosure in Yadav because the result would be an aggregated log of information in Li from multiple computers, including information about the source of the pestware, in a centralized security server described in Yadav. It is my opinion that it would obvious to a POSITA to combine information about the source of pestware from multiple computers in a centralized security server to make correlations between pestware on different computers, and make more accurate determinations whether or not a suspected source of pestware is malicious. A POSITA would have understood that if suspected malware, such as suspected pestware, infected multiple computers from the same source, it would be more likely that that suspected pestware is malicious, rather than if a single computer was infected. Having this aggregated information from multiple computers would allow the system to more

accurately determine if an intrusion is malicious, and would reduce the likelihood of false positives.

194. It would have also been understood to a POSITA in my opinion to combine Li's disclosed UCLog with the centralized security server of Yadav, because it was well known in the art at the time that centralizing activity logs in a common storage location would result in having the benefit of aggregated information about an entire computer network, as opposed to a single computer.

2. Li over Yadav renders obvious Claims 1-14

195. As I explained in Ground 1, Li as modified by Hartrell renders obvious all of the Challenged Claims. As such, for this Ground, I am only addressing those limitations where the disclosures in Hartrell were discussed. My following analysis explains how those grounds discussing the disclosures in Hartrell are also rendered obvious by Li as modified by Yadav.

[1P]: A method for identifying an origin of activity on a computer that is indicative of pestware comprising:

196. To the extent the preamble is limiting, it is my opinion that Li and Yadav teach [1P].

197. In addition to the disclosures in Li that render obvious this limitation, it is my opinion that it would have been obvious for a POSITA to combine the teachings of Li with those in Yadav for the reasons I described above. More

specifically, Yadav discloses that intrusions may include "attempts to gain unauthorized access to data …." EX-1008, 1:45-46. This intrusions of Yadav that may attempt to gain access to data fall within the meaning of pestware, as I explained above.

[1D]: accessing, in response to the identifying an object, at least a portion of a recorded history of externally networked sources that the computer received files from so as to identify a reference to an identity of a particular externally networked source that the suspected pestware object originated from; and

198. In addition to the disclosures in Li that render obvious this limitation, in my opinion, it would have been obvious to combine Li with Yadav for the reasons I previously described. As in Li, Yadav also discloses identifying the source of a particular networked source using at least a portion of a recorded history. For example, Yadav discloses the following:

> When an intrusion prelude is detected, a source of the intrusion prelude is identified (125). For example, a source IP addresses [sic] may be extracted from a packet that is part of the intrusion prelude. This source is then added to a watchlist for increased monitoring (130), and monitoring continues. All packets from the identified source may then be monitored and these packets may be checked for intrusion signature(s). Additionally, multiple sources may be associated with each other, both in intrusion prelude detection and in subsequent intrusion detection, to counter distributed attacks.

EX-1008, 4:31-41. Yadav further discloses identifying the source of a particular networked source using at least a portion of a recorded history in Figure 1 (annotated):

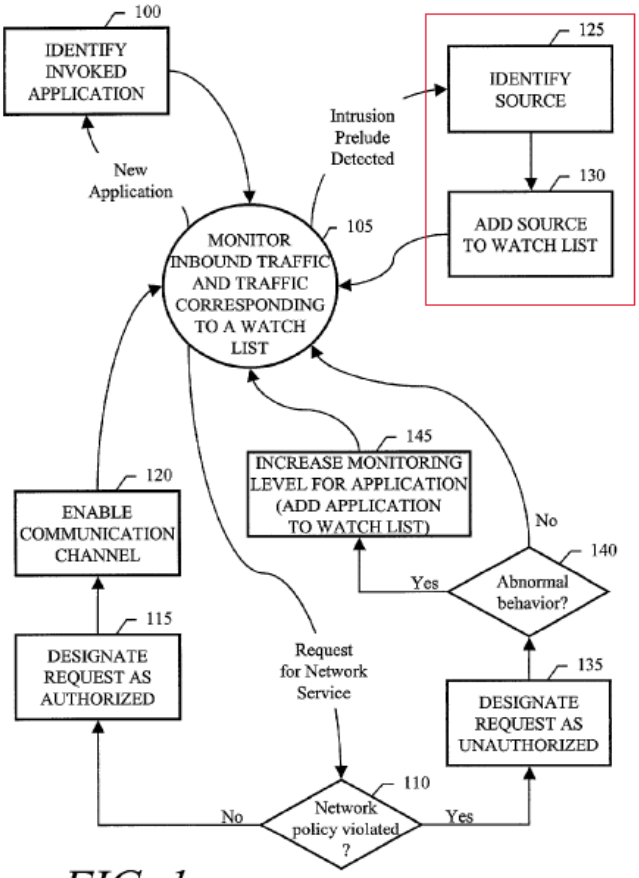

FIG. 1

As such, Yadav discloses the identification of an externally networked source of a detected intrusion from an IP address.

[1E]: reporting the identity of the particular externally networked source to an externally networked pestware research entity so as to enable the externally networked pestware research entity to research whether the particular externally networked source is a source of pestware.

199. For the same reasons as I explained in [1D], Li and Yadav render obvious this limitation.

200. Yadav discloses, for example, that "[i]f the intrusion detector 280 detects an intrusion (*e.g.*, a packet exploit), it may block the traffic and/or report the intrusion to the central security server 292." EX-1006, 10:25-28. It is my opinion that a POSITA would have understood that the reporting of the intrusion in the central security server would have included information pertaining to the detected intrusion, including information about the source of the detected intrusion, as I described *supra* in [1D]. EX-1008, Fig. 1, 4:31-41 ("When an intrusion prelude is detected, a source of the intrusion prelude is identified (125). For example, a source IP addresses [sic] may be extracted from a packet that is part of the intrusion prelude. This source is then added to a watchlist for increased monitoring (130), and monitoring continues. All packets from the identified source may then be monitored and these packets may be checked for intrusion signature(s). Additionally, multiple sources may be associated with each other, both in intrusion prelude detection and in subsequent intrusion detection, to counter distributed attacks.").

201. Moreover, it is also my opinion that a POSITA would have found it obvious to, and have been motivated to, use the source of intrusions detected by various computers in the network that was reported to the central security server, to compare the source of the intrusions detected and check for common sources of the detected intrusions. A POSITA would have understood that doing this would, for

example, allow for the more accurate and specific determination of sources of intrusions. Moreover, a POSITA would have also understood that the central security server disclosed in Yadav would be the externally networked pestware research entity of the '243 Patent, as the central security server is an externally networked pestware research entity that determines whether an externally networked source is a source of pestware. EX-1008, 7:13-18.

202. Moreover, to the extent that "externally networked pestware research entity" is construed broadly to include notifications of detected intrusions being sent to an administrator's computer, it is my opinion that a POSITA would have understood that an administrator could use the central security server disclosed in Yadav to identify the common sources of intrusions described above.

[2A]: wherein the particular externally networked source is identified by an identifier selected from the group consisting of an I.P. address and a URL.

203. As I discussed with respect to [1D] and [1E], the externally networked source identified in Li may be identified by an IP address, as disclosed in Yadav. EX-1008, 4:31-41, Fig. 1. Moreover, and as I previously discussed, Li also discloses identifying an eternally networked source through packet headers, which a POSITA would understand to include IP addresses of an externally networked source. EX-1005, 9, 17. As such, it is my opinion that it would have been obvious to a POSITA to identify an externally networked source using an IP address and/or URL.

Alternatively, it is my opinion that a POSITA would have also found it obvious to identify an externally networked source using an IP address and/or URL, as an IP address and URL are two of the most common ways to refer to networked computers, such as externally networked sources.

[4A]: wherein the recorded history resides in a browser cache, which includes information about files downloaded to the computer and a source of each of the files.

204. In addition to the disclosures in Li, it is my opinion that it would have been obvious to a POSITA to combine the disclosures in Li with those in Yadav for the reasons I already described. Yadav further discloses the following:

> When an intrusion prelude is detected, a source of the intrusion prelude is identified (125). For example, a source IP addresses [sic] may be extracted from a packet that is part of the intrusion prelude. This source is then added to a watch list for increased monitoring (130), and monitoring continues. All packets from the identified source may then be monitored and these packets may be checked for intrusion signature(s). Additionally, multiple sources may be associated with each other, both in intrusion prelude detection and in subsequent intrusion detection, to counter distributed attacks.

EX-1008, 4:31-41. Given this disclosure in Yadav, a POSITA would have understood that it would be possible for the source IP address to be extracted from the browser cache of the monitored computer system, as the browser cache contains information including about recently downloaded files, and the sources of those downloaded files.

205. In my opinion, it would have been obvious to a POSITA that the information disclosed as being collected in Yadav, such as the source IP address from the browser cache, could have been included in the UCLog disclosed in Li. This is because, as I've previously discussed, Li discloses that a single, unified activity log that contains all information collected from a monitored system is more effective in analyzing and identifying intrusions, rather than having separate logs for all monitored information. EX-1005, 1-3. Moreover, it is my opinion that a POSITA would have recognized that a browser cache from a monitored system could contain information relevant to network activity, and would they have been motivated to include such information from a browser cache as part of the UCLog disclosed in Li.

[5A]: wherein the recorded history resides in at least one log selected from the group consisting of an activity log, a browser history, browser cache, browser settings, operating system settings, an event log, a debugging log, a firewall log, file information and monitoring software logs.

206. In the addition to the disclosures in Li, and as discussed *supra* in [4A], it is my opinion that it would have been obvious to a POSITA that the combination of Li in view of Yadav would disclose that part of the recorded history resides in a browser cache.

[6P]: A system for identifying a source of activity on a computer that is indicative of pestware including:

207. To the extent the preamble is limiting, it is my opinion that Li and Yadav teach [6P] for the same reasons as [1P]. Li and Yadav both disclose the implementation of the method described in Claim 1 being performed in a system. For example, Li discloses an "intrusion detection system." EX-1005, 1-2. Moreover, Yadav describes "[a]n integrated intrusion detection system." EX-1008, Abstract.

[6C]: a research portion configured to access, in response to a prompt from a heuristics module, a first set of recorded information on the computer that relates the activity to at least one file residing on the computer, and wherein the research portion is configured to access a second set of recorded information on the computer that relates the at least one file to an externally networked source from which the file was received; and

208. In addition to the disclosures in Li, it is my opinion that it would have been obvious to a POSITA to combine the disclosures in Li with those in Yadav for the reasons I already described. Yadav discloses the process of determining whether there was an intrusion on the monitored system, and then determines additional information about that intrusion, including the identification of the externally networked source of the intrusion. As such, Yadav discloses the following:

> When an intrusion prelude is detected, a source of the intrusion prelude is identified (125). For example, a source IP addresses [sic] may be extracted from a packet that is part of the intrusion prelude. This source is then added to a watch list for increased monitoring (130), and monitoring continues. All packets from the identified source may then be monitored and these packets may be checked for intrusion signature(s). Additionally, multiple sources may be associated with each other, both in intrusion prelude detection and in subsequent intrusion detection, to counter distributed attacks.

EX-1008, 4:31-41. It is my opinion that a POSITA would have understood that the portion of the system of Yadav that determines the additional information about the detected intrusion would be the research portion that performs the other requirements of [6C]. At a minimum, it is my opinion that it would have been obvious to a POSITA that the portion of the system responsible for determining additional information about a suspected intrusion could have been separated into a portion referred to as a "research portion."

209. Moreover, it also is my opinion that it would have been obvious to a POSITA that the determination of additional information about a detected intrusion in Yadav would be performed in response to a prompt from a portion of the system that determines if a file is a potential intrusion. This is because additional information about a file would only need to be collected if a determination is made that that file is an intrusion or potential intrusion. Moreover, this conclusion is further depicted in Figure 1 of Yadav:

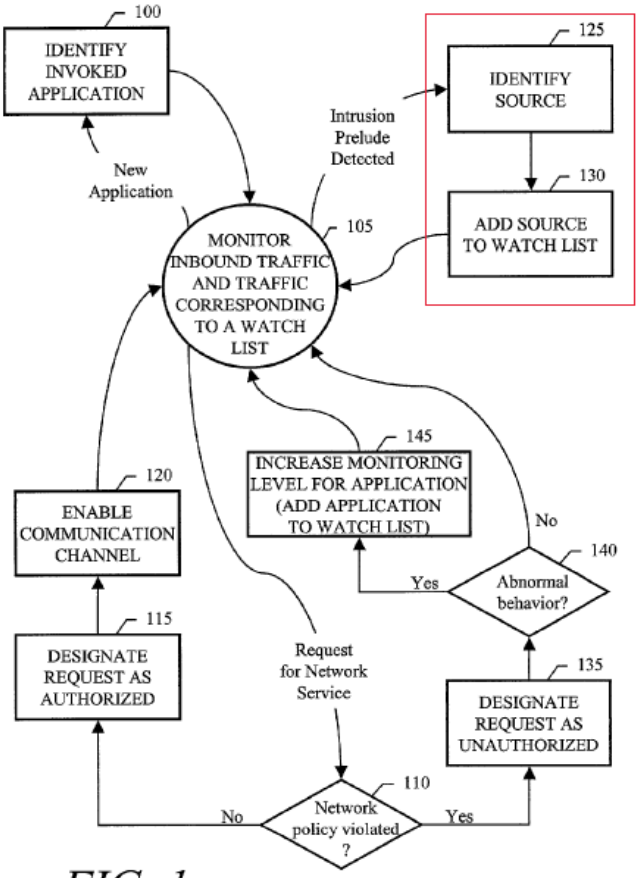

FIG. 1

EX-1008, Fig. 1 (annotated). Indeed, Yadav discloses that once an intrusion preclude is detected by the system, the system will then seek to identify the source of the detected intrusion. *Id.*, 4:31-41. It is therefore my opinion that a POSITA would have at least found it obvious that the research portion would check for additional information about a file, such as its source, in response to a prompt from another portion of the system that is responsible for identifying potential intrusions.

210. Moreover, Yadav explained that the disclosed system will monitor network traffic in order to determine when a potential intrusion has occurred based

upon the flow of that traffic flow, port scanning, and other rules. Indeed, Yadav discloses the following:

> Following the creation of an open channel, inbound traffic that corresponds to the open channel is allowed, whereas inbound traffic that fails to correspond to an open channel is blocked in the monitoring state 105. Moreover, outbound traffic may also be monitored in the monitoring state 105, and disabled channels may also be created, such as by using the deny action discussed above. Blocked traffic is monitored to detect an intrusion prelude, for example, a system scan, a port scan and/or an operating system (OS) fingerprinting. The blocked traffic may be checked for patterns that span multiple communications and/or multiple communication channels (e.g., multiple TCP/IP (Transmission Control Protocol/Internet Protocol) connections).

Id., 4:18-30. Given this disclosure, it would have been obvious to a POSITA, in my opinion, that the set of network events (*i.e.*, the first set of recorded information) would be accessed by the system in order to determine if there was a potential intrusion, and flag it accordingly. It would have also been obvious to a POSITA that, in determining additional information about a file that has been determined to be an intrusion or potential intrusion, that the system would access a second set of recorded information, such as the "network events," in order to determine additional information about the intrusion, like the externally networked source of the intrusion.

[6D]:a reporting portion configured to generate a report that identifies the externally networked source of the file and to report an identity of the externally networked source to an externally networked pestware research

entity so as to enable the externally networked pestware research entity to research whether the externally networked source is a source of pestware.

211. It is my opinion that Li and Yadav teach [6D] for the same reasons they teach [1E].

212. Moreover, it is my opinion that a POSITA would have understood that when the system in Yadav reports information to a central security server, it must generate a report with that relevant information, which would include at least the determined source of that intrusion. That report, which is sent to the central security server (*i.e.*, the externally networked pestware research entity), would then use that information to compare against the information stored in the server from other computers, to determine whether the networked source is a source of an intrusion, like pestware. It is my opinion that a POSITA would have found it obvious that the portion that generates this report of information pertaining to the potential intrusion could be separated into a reporting portion of the code. It is therefore my opinion that Li in view of Yadav render obvious this limitation.

[12P]: A non-transitory computer-readable medium including processor-executable instructions for identifying an origin of activity on a computer that is indicative of pestware, the instructions including instructions for:

213. To the extent the preamble is limiting, it is my opinion that Li and Yadav teach [12P] for the same reasons they teach [1P].

214. Li and Yadav both disclose implementing the process described in [1P] using a non-transitory computer-readable medium. For example, Li explains that the disclosed UCLog system was implemented "on a real system running Microsoft Outlook Express on Windows 2000;" *e.g.*, software. EX-1005, 3. Moreover, Yadav discloses that the disclosed system uses memory and other storage. EX-1008, 9:60-65 ("The data processing system 600 includes a memory 620, which may be volatile and/or non-volatile memory, and is coupled with the communications bus 615. The system 600 may also include one or more cache memories. These memory devices enable storage of instructions and data close to the central processor 610 for retrieval and execution.").

F. Ground 4: Claims 1-14 are obvious under §103 over Li and Yadav, and Mandujano.

215. To the extent that Li and Yadav do not render obvious every limitation of the Challenged Claims, it is my opinion that the Challenged Claims would be rendered obvious in view of Li, Yadav, and Mandujano.

1. Motivation to Combine and Reasonable Expectation of Success

216. It is my opinion that a POSITA would have been motivated to combine the teachings of Li and Yadav with Mandujano for the same reasons it is my opinion that a POSITA would have been motivated to combine Li, Hartrell, and Mandujano

in Section VII.D.1. It is my opinion that there would have not been any differences in the motivation between Li as modified by Hartrell, and Li as modified by Yadav.

2. Li over Yadav and Mandujano render obvious limitations [1B] and [1C]

217. To the extent that Li and Yadav do not render obvious these limitations, it is my opinion that Li, Yadav, and Mandujano disclose [1B] and [1C]. As I previously discussed *supra* in Section VII.D.2, Mandujano discloses the use of a "score-based system" to determine whether or not an object is malware. EX-1007, 106. It is my opinion that it would have been obvious to combine Li and Yadav with Mandujano for the reasons I set forth *supra* in Section VII.D.2. As such, it is my opinion that Claim 1 and its dependent limitations are rendered obvious over Li, Yadav, and Mandujano.

3. Li over Yadav and Mandujano render obvious limitation [6B]

218. To the extent that Li and Yadav do not render obvious this limitation, it is my opinion that Li, Yadav, and Mandujano teach [6B] for the same reasons they teach [1B] and [1C]. Additionally, as I discussed *supra* in [1B] and [1C], Li, Yadav, and Mandujano all disclose using heuristics (*i.e.*, rules) for identifying activity that is indicative of an intrusion, such as pestware, based on weighted factors and a threshold. It is my opinion that it would have obvious to a POSITA for the reasons

described *supra* in Section VII.D.3. As such, it is my opinion that Claim 6 and its dependent limitations are rendered obvious over Li, Yadav, and Mandujano.

4. Li over Yadav and Mandujano render obvious limitations [12B] and [12C]

219. It is my opinion that Li, Yadav, and Mandujano teach [12B] and [12C] for the same reasons that they teach [1B] and [1C]. Therefore, it is my opinion that Claim 12 and its dependent limitations are all rendered obvious in view of Li, Yadav, and Mandujano.

VIII. SECONDARY CONSIDERATIONS

220. I am not aware of any evidence of secondary considerations of non-obviousness relied upon by Webroot. To the extent Webroot is permitted to provide any evidence of secondary considerations to rebut my opinions expressed herein, I reserve the right to respond by supplementing and/or amending this declaration or submitting a reply declaration to consider the alleged secondary considerations of non-obviousness.

IX. RIGHT TO SUPPLEMENT

221. I reserve the right to supplement this declaration, if appropriate, should additional information come to light that is relevant to my opinions in this declaration. I also reserve the right to consider and comment on additional evidence,

e.g., objective evidence of non-obviousness, that may be presented by Webroot or its experts.

222. At any trial or hearing at which I may testify in this matter, I may provide demonstrative aids, such as computer animations, excerpts, and figures from relevant exhibits and prior-art references, and physical examples to assist in explaining the subject matter in my report.

223. I will continue my study and evaluation of relevant prior art as these proceedings continue, at least up until the end of the period prescribed by the relevant rules and regulations. In the event further issues arise that concern the subject matter in my declaration or additional information becomes available, I expressly reserve the right to supplement and/or amend my opinions as stated in this declaration as well as the bases supporting my opinions. I specifically reserve the right to supplement and/or amend this declaration at such time that the Board defines the disputed terms in the Challenged Claims, particularly if the Board adopts alternate instructions not advanced by Petitioners. I further reserve the right to supplement and/or amend this declaration to submit a reply declaration based on any information or contentions expressed by Webroot or its experts attempting to rebut my opinions in this declaration. In addition, I reserve the right to use demonstratives or other

exhibits at trial in support of my opinions in any of my expert declarations and/or supplements thereto.

X. CONCLUSION

224. For the reasons set forth above, it is my opinion that the Challenged Claims of the ’243 Patent are invalid.

Executed on April 3, 2023
Lexington, MA

By: Henry Houh.
Dr. Henry Houh