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. IPR2023-00732

U.S. Patent No. 8,719,932

---

Petition for *Inter Partes* Review of U.S. Patent No. 8,719,932

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 CONTENTS**

**Page**

I. INTRODUCTION ..... 1

II. MANDATORY NOTICES ..... 2

A. Real Parties-in-Interest 37 C.F.R. § 42.8(b)(1) ..... 2
B. Related Matters Under 37 C.F.R. § 42.8(b)(2) ..... 2
C. Lead and Backup Counsel ..... 2
D. Service of Information Under 37 C.F.R. § 42.8(b)(4) ..... 4

III. PAYMENT OF FEES ..... 4

IV. REQUIREMENTS OF *INTER PARTES* REVIEW ..... 5

A. Standing ..... 5
B. Identification of Challenge and Relief Requested ..... 5
C. How the Challenged Claims Are to Be Construed Under 37 C.F.R. § 42.104(b)(3) ..... 7
D. How the Challenged Claims Are Unpatentable Under 37 C.F.R. § 42.104(b)(4) ..... 9
E. Supporting Evidence Under 37 C.F.R. § 42.104(b)(5) ..... 9

V. THRESHOLD REQUIREMENT FOR *INTER PARTES* REVIEW ..... 9

VI. PERSON OF ORDINARY SKILL IN THE ART ..... 10

VII. STATE OF THE ART ..... 10

VIII. OVERVIEW OF THE ’932 PATENT ..... 11

IX. DETAILED CHALLENGE ..... 14

A. Ground 1: Claims 1-15 are obvious under §103 over Li and Hartrell ..... 14
B. Ground 2: Claims 1-15 are obvious under § 103 over Li, Hartrell, and Mandujano. ..... 46
C. Ground 3: Claims 1-15 are obvious under §103 over Li and Yadav ..... 55
D. Grounds 4: Claims 1-15 are obvious under §103 over Li, Yadav, and Mandujano. ..... 65



IPR2023-01051
CrowdStrike EX1015 Page 2

**TABLE OF CONTENTS**
(continued)

**Page**

X. PTAB DISCRETION SHOULD NOT PRECLUDE INSTITUTION.....67

A. PTAB should not exercise its discretion to deny institution under *Fintiv*. .....67

B. PTAB should not exercise its discretion to deny institution under *Becton* and *Advanced Bionics*. .....75

XI. CONCLUSION.....75

XII. CERTIFICATE OF WORD COUNT .....77

## TABLE OF AUTHORITIES

**Page(s)**

**Cases**

*10X Genomics, Inc. v. Bio-Rad Labs., Inc.*,
IPR2020-00086, Paper 8 at 17–22 (PTAB Apr. 27, 2020) .....8

*Advanced Bionics LLC v. MED-EL Elektromedizinische Gerate GmbH*,
IPR2019-01469, Paper 6 (PTAB Feb. 13, 2020).....75

*Apple Inc. v. Fintiv, Inc.*,
IPR 2020-00019, Paper 15 (May 13, 2020).....68, 74

*Apple v. Seven Networks*,
IPR2020-00255, Paper 13 (July 28, 2020) .....72

*Becton, Dickinson & Co. v. B. Braun Melsungen AG*,
IPR2017-01586, Paper 8 (Dec. 15, 2017) .....75

*Cizion, LLC v. Kerr Machine Co.*,
PGR2020-00065, Paper 10 (Dec. 3, 2020).....70

*HTC Corp. v. Cellular Communications Equip., LLC*,
877 F.3d 1361 (Fed. Cir. 2017) .....7

*Micron Tech., Inc. v. Godo Kaisha IP Bridge 1*,
IPR2020-01008, Paper 10 (Dec. 7, 2020) .....70

*Mylan Pharm. Inc. v. Sanofi-Aventis Deutschland GMBH*,
IPR2018-01680, Paper 22 (Apr. 3, 2019).....70

*Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*,
868 F.3d 1013 (Fed. Cir. 2017) .....8, 9

**TABLE OF AUTHORITIES**
(continued)

**Page(s)**

*Oticon Medical AB v. Cochlear Ltd.*,
IPR2019-00975 Paper 15 (PTAB Oct. 16, 2019) ..... 75

*Samsung Elec.'s Co., Ltd. et all v. Staton Techniya, LLC*,
IPR2022-00302, Paper 13 (PTAB July 11, 2022) ..... 72

*Sand Revolution II, LLC v. Continental Intermodal Grp.*,
IPR2019-01393, Paper 24 (June 16, 2020) ..... 68, 73

*Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*,
200 F.3d 795 (Fed. Cir. 1999) ..... 8

*VMware Inc. v. Intellectual Ventures II LLC*,
IPR2020-00859, Paper 13 (Nov. 5, 2020) ..... 68

*Volkswagen Grp. of Am., Inc. v. Arigna Tech. Ltd.*,
IPR2021-01321, Paper 10 (Feb. 15, 2022) ..... 68

*Webroot, Inc. v. AO Kaspersky Lab*,
No. 6:22-cv-00243-ADA-DTG (W.D. Tex.) ..... 71, 74

*Western Digital Corp. v. Kuster*,
IPR2020-01391, Paper 10 (Feb. 16, 2021) ..... 68

*Western Digital Corp. v. SPEX Techs., Inc.*,
IPR2018-00082, Paper 11 (PTAB Apr. 25, 2018) ..... 8

**Other Authorities**

https://www.uspto.gov/sites/default/files/documents/interim_proc_discretionary_denials_aia_parallel_district_court_litigation_memo_20220621_.pdf ..... 72

**TABLE OF AUTHORITIES**
(continued)

**Page(s)**

*PTAB Consolidated Trial Practice Guide* 59 (Nov. 2019).....74

## TABLE OF EXHIBITS

| Exhibit Number | Document |
|---|---|
| 1001 | U.S. Patent No. 8,719,932 ("the '932 Patent") |
| 1002 | File History of the '932 Patent |
| 1003 | Declaration of Dr. Henry Houh |
| 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")[1] |
| 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 | Webroot October 25, 2022 Infringement Contentions |
| 1011 | Reserved |

[1] Numerical citations to EX-1005 herein refer to column numbers added by Petitioners for the sake of specificity.

**TABLE OF EXHIBITS**
(continued)

| Exhibit Number | Document |
|---|---|
| 1012 | Reserved |
| 1013 | Reserved |
| 1014 | Reserved |
| 1015 | Reserved |
| 1016 | Stipulation Waiving IPR Claims in District Court Litigation |
| 1017 | Excerpt from Transcript of Motions Hearing in *Webroot, Inc., et al. v. AO Kaspersky Lab*, No. 6:22-cv-00243-ADA-DTG (W.D. Tex.) (Dec. 9, 2022) |

## I. INTRODUCTION

Sophos Ltd. and Sophos Inc. petition for *inter partes* review (IPR), seeking cancellation of claims 1-15 of U.S. Patent No. 8,719,932 ("the '932 Patent," EX-1001). This petition demonstrates that there is at least a reasonable likelihood that Petitioners will prevail on at least one challenged claim based upon prior-art references that the USPTO did not have before it during prosecution.

The '932 Patent describes and claims collecting information about system events on a computer, analyzing those events for potential "pestware" (*i.e.*, software that collects information about a person or an organization, including "malware" or "spyware") and reporting the source of that pestware. The patent acknowledges that there was already software available to detect and remove pestware, but purports to add the ability to determine and report the source of the pestware, based on information gathered pertaining to the pestware.

None of this was new. As demonstrated below, existing systems were already analyzing computer events to determine and report the source of the detected pestware. Claims 1-15, therefore, should be cancelled as unpatentable under 35 U.S.C. §103.

## II. MANDATORY NOTICES

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

Sophos Ltd., and Sophos, Inc. are the real parties-in-interest.

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

#### 1. Current Litigation

The '932 Patent is the subject of five pending litigations in a suit brought by Patent Owner against Sophos Ltd. and four other defendants. *Webroot, Inc. v. Sophos Ltd.*, No. 6:22-cv-00240-ADA-DTG (W.D. Tex.), Dkt. No. 1 (the "District Court Action"), *Webroot, Inc. v. Forcepoint LLC*, No. 6:22-cv-00342-ADA-DTG (W.D. Tex.), Dkt. No. 1, *Webroot, Inc. v. Trend Micro, Inc.*, 6:22-cv-00239-ADA-DTG (W.D. Tex.), Dkt. No. 1, *Webroot, Inc. v. CrowdStrike Holdings, Inc.*, 6:22-cv-00241-ADA-DTG (W.D. Tex.), Dkt. No. 1, *Webroot, Inc. v. AO Kaspersky Lab*, 6:22-cv-00243-ADA-DTG (W.D. Tex.), Dkt. No. 1. These cases are now consolidated as *Webroot, Inc. v. AO Kaspersky Lab*, No. 6:22-cv-00243-ADA-DTG (W.D. Tex.).

#### 2. Administrative Proceedings

There are no other administrative proceedings at issue.

### C. Lead and Backup Counsel

Petitioners designate the following counsel:

| Lead Counsel | Backup Counsel |
|---|---|
| Ryan Iwahashi<br>(Reg. No. 63,378)<br>Gibson, Dunn & Crutcher LLP<br>1881 Page Mill Road<br>Palo Alto, CA 94304-1211<br>Tel: (650) 849-5367<br>RIwahashi@gibsondunn.com | Josh Krevitt<br>(*pro hac vice* motion requested)<br>Gibson, Dunn & Crutcher LLP<br>1881 Page Mill Road<br>Palo Alto, CA 94304-1211<br>Tel: (212) 351-2490<br>JKrevitt@gibsondunn.com |
| | Brian A. Rosenthal<br>(*pro hac vice* motion requested)<br>Gibson, Dunn & Crutcher LLP<br>200 Park Avenue<br>New York, NY 10166-0193<br>Tel: (212) 351-2339<br>BRosenthal@gibsondunn.com |
| | Timothy P. Best<br>(*pro hac vice* motion requested)<br>Gibson, Dunn & Crutcher LLP<br>333 South Grand Avenue<br>Los Angeles, California 90071-1504<br>Tel: (213) 229-7659<br>TBest@gibsondunn.com |
| | Kate Dominguez<br>(*pro hac vice* motion requested)<br>Gibson, Dunn & Crutcher LLP<br>200 Park Avenue<br>New York, NY 10166-0193<br>Tel: (212) 351-2338<br>KDominguez@gibsondunn.com |

Petitioners respectfully request authorization to file motions for Josh Krevitt, Brian Rosenthal, Kate Dominguez, and Timothy Best to appear before the USPTO *pro hac vice*. Mr. Krevitt, Mr. Rosenthal, Ms. Dominguez, and Mr. Best are experienced litigating attorneys and are currently serving as lead counsel for Petitioners in the District Court Action. Each has established familiarity with the subject matter of this proceeding. Petitioners intend to file a motion to appear *pro hac vice* under 37 C.F.R. § 42.10. Pursuant to 37 C.F.R. § 42.10(b), powers of attorney accompany this petition.

### D. Service of Information Under 37 C.F.R. § 42.8(b)(4)

Service of any documents via hand delivery may be made at the mailing address of lead and backup counsel designated above. Petitioners also hereby consent to electronic service, and service via electronic mail may be made at the email addresses provided above for the lead and backup counsel.

## III. PAYMENT OF FEES

Pursuant to 37 C.F.R. §§42.103 and 42.15(a), the required fee is submitted herewith. The Office is authorized to charge any fee deficiency, or credit overpayment, to Deposit Account 50-1408. Additional fees due in connection with this petition may be charged to the foregoing account.

## IV. REQUIREMENTS OF *INTER PARTES* REVIEW

### A. Standing

Pursuant to 37 C.F.R. §42.104(a), Petitioners certify that the '932 Patent is available for IPR and that Petitioners are not barred or estopped from requesting IPR of the claims on the grounds identified herein. Specifically, Petitioners certify the following: Petitioners have not filed a civil action challenging the validity of the '932 Patent; this petition is filed not more than one year from October 4, 2022, the date on which the Sophos Ltd. received service of the complaint alleging infringement of the '932 Patent; the estoppel provisions of 35 U.S.C. §315(e)(1) do not prohibit this *inter partes* review; and this petition is filed after the later of (a) the date that is nine months after the date of the grant of the '932 Patent or (b) the termination of any post-grant review of the '932 Patent.

### B. Identification of Challenge and Relief Requested

Pursuant to 37 C.F.R. §42.104(b), Petitioners request that the Board institute IPR of claims 1-15 (the "Challenged Claims") of the '932 Patent on one or more

grounds under 35 U.S.C. § 103.[2] The precise relief that Petitioners request is that claims 1-15 be cancelled in view of the following prior art references:

| Reference | Qualifying Date | Prior Art Under |
|---|---|---|
| Li | January 31, 2005 | §102(b) |
| Hartrell | December 28, 2005 | §102(e) |
| Mandujano | December 9, 2004 | §102(b) |
| Yadav | August 7, 2003 | §102(b) |

The ’932 Patent is a U.S. patent resulting from Application No. 13/490,294, which was filed on June 6, 2012. The application claims priority to application No. 11/408,243, now U.S. Patent No. 8,201,243, which was filed on April 20, 2006. In the district court litigation, moreover, Patent Owner asserted a priority date of April 20, 2006. EX-1010 (Webroot October 25, 2022 Infringement Contentions), 7. Petitioners therefore assume that the Challenged Claims are entitled to a priority date of April 20, 2006 for the purposes of this petition, without waiving its right to challenge that priority date in any proceeding.

[2] The application that issued as the ’721 Patent was filed before March 16, 2013, and thus is subject to the pre-AIA versions of 35 U.S.C. §§ 102 and 103, and thus all references to Sections 102 and 103 refer to their pre-AIA versions.

Each of the references cited above is prior art. Li was published at least by January 31, 2005, and thus is prior art at least under §102(b). EX-1009, ¶¶43-44. Hartrell was filed on December 28, 2005 and is prior art under §102(e). Mandujano was published by December 9, 2004, and is prior art under §102(b). EX-1009, ¶¶39, 44. Yadav was filed on February 1, 2002 and published August 7, 2003, and is therefore prior art under §102(b). None of these prior art references was cited during the prosecution of the application that issued as the '932 Patent. *See, e.g.*, Ex-1001 at 1 (listing references cited). The Challenged Claims are unpatentable based on the following:

| Ground | Claims | Basis for Rejection |
|---|---|---|
| 1 | 1-15 | §103 by Li in view of Hartrell |
| 2 | 1-15 | §103 by Li in view of Hartrell and Mandujano |
| 3 | 1-15 | §103 by Li in view of Yadav |
| 4 | 1-15 | §103 by Li in view of Yadav and Mandujano |

### C. How the Challenged Claims Are to Be Construed Under 37 C.F.R. § 42.104(b)(3)

Petitioners do not believe any constructions have an impact on the invalidity analyses set forth herein. *See HTC Corp. v. Cellular Communications Equip., LLC*, 877 F.3d 1361, 1367–68 (Fed. Cir. 2017) (affirming the Board's application, absent

an express construction of a term). Although Petitioners and Patent Owner disagree over the construction of certain terms in the parallel District Court litigation, for the purpose of this Petition, Petitioners rely on Patent Owner's proposed constructions (plain and ordinary meaning). *See 10X Genomics, Inc. v. Bio-Rad Labs., Inc.*, IPR2020-00086, Paper 8 at 17–22 (PTAB Apr. 27, 2020) (instituting IPR and clarifying that a Petitioner need only identify "[h]ow the challenged claim is to be construed" for purposes of the petition and that "judicial efficiency will be enhanced by allowing Petitioner to rely upon a claim construction that Patent Owner is relying upon in the related district court litigation to assert infringement of the challenged patent"); *see also Western Digital Corp. v. SPEX Techs., Inc.*, IPR2018-00082, Paper 11 at 12 (PTAB Apr. 25, 2018) ("Petitioner's statement that its Petition 'is *based on* the claim constructions urged by Patent Owner' in related District Court litigation . . . suffices to identify claim constructions Petitioner is adopting for purposes of the requested review in compliance with §104(b)(3).").

Moreover, the Board "need only construe terms 'that are in controversy, and only to the extent necessary to resolve the controversy.'" *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)).

Because Petitioners base this Petition on constructions *Patent Owner* has advocated, the Petition does not present any controversy over claim meaning and the Board need not construe any terms. *Nidec*, 868 F.3d at 1017.

### D. How the Challenged Claims Are Unpatentable Under 37 C.F.R. § 42.104(b)(4)

An explanation of how the Challenged Claims are unpatentable, including the identification of where each element of the claim is found in the prior art patents or printed publications, is provided below.

### E. Supporting Evidence Under 37 C.F.R. § 42.104(b)(5)

The exhibit numbers of the supporting evidence relied upon and the relevance of the evidence to the Challenged Claims, including an identification of specific portions of the evidence that support the challenge, are provided below. A List of Exhibits identifying the exhibits is also included in this petition pursuant to 37 C.F.R. § 42.63(e). The technical information and grounds for rejection explained in the petition are further supported by the Expert Declaration of Henry Houh, attached as Exhibit 1003.

## V. THRESHOLD REQUIREMENT FOR *INTER PARTES* REVIEW

Under 35 U.S.C. § 314(a), institution of *inter partes* review requires "a reasonable likelihood that the petitioners would prevail with respect to at least one

of the claims challenged in the petition." This Petition meets this threshold for each ground.

## VI. PERSON OF ORDINARY SKILL IN THE ART

A person of ordinary skill in the art ("POSITA") in April 2006 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. EX-1003 ¶36. Alternately, more education could substitute for less work experience and vice versa. *Id*. A POSITA would either have six months' experience as a network or system administrator, or have taken two advanced computer-security courses. *Id.*

## VII. STATE OF THE ART

As of April 2006, it was well known by POSITAs and the general public alike that computers connected to the internet were subject to attacks by malicious software, such as viruses, worms, trojan horses, and other software-based attacks. EX-1003 ¶54-55. These types of attacks were well-known and there were many anti-virus programs to prevent or detect and remove malware and pestware from a user's computer. *Id*. Indeed, as the '932 patent acknowledges, at the time of the

alleged invention, software was "available to detect and remove pestware." EX-1001, 1:55-56.

## VIII. OVERVIEW OF THE '932 PATENT

The '932 patent generally relates to "researching an identity of a source of activity that is indicative of pestware." EX-1001, Abstract. The patent seeks to protect against malicious software, such as "trojans, spyware, and adware," which are "collectively referred to as 'malware,' 'spyware,' or 'pestware'." The patent asserts that prior art systems rely upon "definitions of known pestware to search for and remove files," and it may be difficult to "initially locate the pestware in order to create the definitions." *Id.*, 2:3-8.

To address the alleged shortfalls, the patent purports to describe and claim a system that can identify pestware by monitoring activity on a computer and then analyzing recorded information on the computer (e.g., "an event log", "a debugging log", "a firewall log" and others (*id.*, 6:28-34)) to determine "the identities (e.g., I.P. address, URL…) of sources (e.g., web sites…) of the pestware." *Id.*, 3:53-55. In other words, the '932 patent describes monitoring to identify the presence of pestware, and correlating the activity with other recorded logs to identify a source, such as an IP address or URL, of the intrusion. Figure 4 is illustrative.

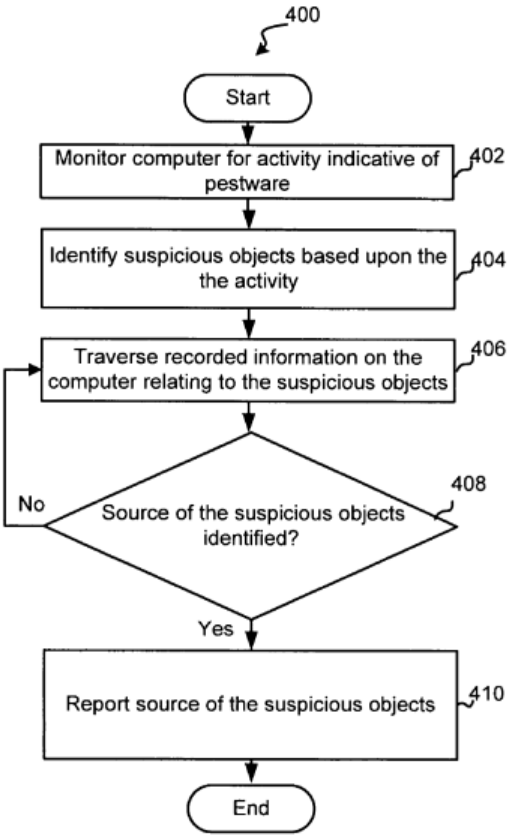


**FIGURE 4**

The method shown in Figure 4 monitors a computer for activity indicative of pestware **402** and identifies suspicious objects **404** based on that activity. *Id*., 8:16-33. The method then checks recorded information on the computer **406** to determine the source of the suspicious objects **408**. *Id*., 8:34-42. If the source is identified, it will report that source **410** "e.g., to a pestware research entity" *Id*., 8:34-35, for

example, "a centralized location where the URLs may be added to a list of 'bad URLs.'" *Id*., 8:5-15. The challenged claims generally follow these five steps:

1) monitor the computer for pestware activity;
2) analyze computer activity to determine whether activity is pestware activity;
3) identify suspected pestware objects based upon the activity;
4) access historical logs to identify the source of the suspected pestware; and
5) report the source of the pestware. *Id*., cls. 1, 6, 12.

During prosecution of the parent application, the applicant made two additions to the claims to overcome prior art rejections, which are also in the Challenged Claims. First, the 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, the applicant added the "reporting" limitation, requiring that the externally networked source is 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). The '243 patent's specification does not specifically mention an "externally networked" source or "externally networked" research entity. The specification briefly mentions a "research entity" twice with no details about implementation. EX-1001, 8:35-38; 9:50-52; EX-1003, ¶57.

## IX. DETAILED CHALLENGE

### A. Ground 1: Claims 1-15 are obvious under §103 over Li and Hartrell.

Li and Hartrell render obvious every limitation of claims 1-15.

#### 1. Prior Art Overview

Li was published by January 31, 2005 as part of the proceedings of the 12th International Conference on Telecommunication Systems-Modeling and Analysis (ICTSM). EX-1005; EX-1009, ¶¶43-44. Li, therefore, qualifies as prior art under 35 U.S.C. §102(b). Li describes a system for detecting intrusions using a "unified logging architecture" that correlates logs from heterogeneous sources. EX-1005, 1. Like the '243 patent, Li explains that prior art intrusion detection systems detected attacks using manually defined signature definitions and did not correlate

information recorded by different logging components, such as "tcpdump logs" or "system call logs." *Id*., 2. To remedy this issue, Li discloses a "Unified, Correlated Logging Architecture," abbreviated as "UCLog," that 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 further discloses analyzing the computer activity to identify abnormal activity based upon a heuristic algorithm and a threshold. *Id*., 6-7. Once an intrusion is detected, Li discloses tracing the log back to identify the source and execution path of the intrusion. *Id*., 13.

Hartrell was filed December 28, 2005 and issued on February 14, 2012. EX-1006. Hartrell, therefore, qualifies as prior art under 35 U.S.C. §102(e). Hartrell describes a "malware analysis system for automating cause and effect analysis of malware infections." *Id*., Abstract. Hartrell explains that a problem with current systems for detecting malware, such as "spyware," is that "system administrators are unable to determine the root cause or origin of that malicious code." *Id*., 1:23-46. To resolve this problem, Hartrell describes a system with a "remote (e.g., centralized) data store" *Id*., 2:51 that receives "snapshots" of "local system and network activity" from monitored computers when malware is detected. *Id*., 3:38-

53, 10:23-50. The centralized data store uses the information 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.*

### 2. Motivation to Combine and Reasonable Expectation of Success

A POSITA would have been motivated to combine the teachings of Li and Hartrell for multiple reasons, including to produce the obvious, beneficial, and predictable result of facilitating the broad-scale implementation of Li, including by consolidating information of potential threats across multiple computers in a network. EX-1003 ¶81.

When considering the teachings of Li, a POSITA would also have been motivated to consider the teachings of Hartrell, since Li and Hartrell both pertain to the same field of endeavor of intrusion detection and prevention. EX-1003 ¶82. Li describes an intrusion detection system with a unified log architecture used to track intrusions back to their source. EX-1005, 13. Hartrell also describes a malware detection system that traces back malware to its source, including sending source information to a centralized server where it can be tracked and aggregated for

different computers across a network. EX-1006; *see also* EX-1003 ¶82. For these reasons, Li and Hartrell are in the same field of endeavor and are analogous to the claimed invention of the '243 Patent.

Moreover, a POSITA would have been motivated to combine the teachings of Li and Hartrell to obtain predictable and beneficial results. EX-1003 ¶¶83. As explained above, Li describes creating a unified log of system and network events on a computer, and that "[d]istributed loggers are very useful and can be implemented to log system-wide information." Li states: "Obtaining a system-wide view is very helpful for intrusion detection, and related malicious activities may appear in several hosts." EX-1005, 10-11. Hartrell likewise describes combining information from multiple logging components on multiple computers in a centralized store so as to make malware determinations with information from multiple computers. A POSITA would have known to modify Li in view of the teachings of Hartrell because doing so would aggregate the system-wide unified log information disclosed in Li within the centralized database described in Hartrell. EX-1003 ¶83. A POSITA would have understood that, if pestware infected multiple computers after network communication with the same source that the source is more likely to be malicious than if only a single computer was infected and therefore

would reduce the likelihood of incorrectly identifying a source as malicious (*i.e.*, a false positive). *Id*.

### 3. Analysis

#### a) Claim 1

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

To the extent the preamble is limiting, Li discloses [1P]. EX-1003, ¶84. Li discloses identifying the origin (or source) of intrusive software (such as pestware) on a computer, explaining 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; *id*., 2 ("At an intrusion, UCLog can be used to ***automatically identify the source and the execution path*** of the intrusion."); EX-1003 ¶84-85. Li explains that the intrusions the disclosed system is designed to detect include different types of malware, including viruses and worms. EX-1005, 2. Li uses the Yaha virus as an example, which "reads the address book and sends itself to the contacts." *Id*., 20. A POSITA would have understood that the Yaha virus collects information about a person (e.g., contacts in the address book) and therefore is an example of pestware, as described by the patent or under any other possible construction of "pestware." *Id*.; EX-1001, 1:58-61 ("Unless specified

otherwise, 'pestware' as used herein refers to any of these programs that collects information about a person or an organization."); EX-1003, ¶86.

Li in view of Hartrell also discloses [1P]. EX-1003 ¶88. It would have been obvious to modify Li in view of Hartrell for the reasons described above, and Hartrell also discloses detecting the source of potential malicious software. EX-1006, 2:51-57 ("The 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."). Hartrell states that infection can occur when "a user uses the computer system to visit a **source** of the malware, such as a web site." EX-1006, 7:21-23. Hartrell describes "spyware" as a form of "malicious infection." EX-1006, 1:23-26, 10:22-50; EX-1003, ¶88. It therefore would have been obvious to a POSITA that the intrusion detection system described in Li as modified by Hartrell was capable of identifying the source or origin of activity of pestware on a computer, and a POSITA would have been motivated to use it for that purpose. *Id*.

**[1A]: monitoring, using a kernel-mode driver, API call activity on the computer;**

Li discloses [1A]. EX-1003, ¶89.

In Li, "[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. Monitors "are responsible for filtering and classifying the stream entries, and detecting any abnormal behavior." *Id.*, 11. Li describes a Kernel API Logger: "A kernel API logger should record system calls, the parameters of those calls, and the time at which they are made." *Id.*, 9. A POSITA therefore would have understood that the Kernel API Logger was providing kernel API activity to the monitor, and that data from the monitor would be stored in an "activity database" that "stores and manages audit data." *Id.*, 12.l EX-1003, ¶90. Li also explains that "[e]ach logging module must be coupled with the subsystem from which the logger is collecting audit data." A POSITA therefore would have understood that the most straightforward way to implement a kernel API activity logger would be a kernel-mode driver, so that it would be "coupled with" the kernel API subsystem. Li also mentions using loggers like WinDump and FileMon, which would use kernel-mode drivers. EX-1003, ¶91. A POSITA would have known that without kernel access,

such as via a kernel-mode driver, the monitor would not have been able to ensure that it tracks all kernel API calls. *Id.* Moreover, as discussed *supra* in [1PRE], Li discloses monitoring for computer activity indicative of pestware and other types of intrusions. EX-1003, ¶85.

**[1B]: storing information related to the API call activity in a log;**

Li discloses [1B]. EX-1003, ¶92.

As in [1A], Li discloses storing API call activity and information about those APIs in UCLog. EX-1005, 9; EX-1003, ¶90.

**[1C]: analyzing, heuristically, the API call activity to determine whether one or more weighted factors associated with the API call activity exceeds a threshold;**

Li discloses [1C]. EX-1003, ¶94.

Li discloses using a set of rules (heuristics) to determine whether activity on a computer is indicative of an intrusion (e.g., pestware) when it meets a specific "threshold for abnormality." EX-1005, 19; EX-1003, ¶95. For example, Li discloses "obtaining the rules from the training data" and then analyzing "each sequence of system calls" to predict if that sequence is "'normal' or '***abnormal***' according to the rules." EX-1005, 6. "If the number of abnormal prediction in a region is ***greater than a half***, we predict the region as 'abnormal.'" *Id.*, 6-7. In short, Li discloses analyzing, using a set of rules, monitored computer activity using

the logs (a sequence of system calls) to determine heuristically whether one or more factors (different input data) meet a certain threshold (e.g., more than 50%) to determine if the activity is indicative of an intrusion (e.g., pestware). EX-1003, ¶95. "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." EX-1005, 20. It would have been obvious to a POSITA that using a training algorithm, the different factors could have each been weighted differently, depending on how likely those factors are to indicate an intrusion. EX-1003, ¶95. A POSITA would therefore have been motivated to weigh each factor differently in the rules/heuristics calculations to make the determination as to whether the activity is indicative of an intrusion accurate. *Id*.

Alternatively, it would have been obvious to a POSITA that the rules set forth in Li could be based upon factors such as, an "abnormal increase in the network traffic," or number of "file I/O." EX-1005, 7, 19-20; EX-1003, ¶ 96. For example, Li states "[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." EX-1005, 20. A POSITA would have understood that there are many different factors that may be indicative of an intrusion like pestware, including abnormal increases in network traffic, number of file input/outputs, and registry modifications. EX-1003, ¶96. Although each of these factors may be indicative of an intrusion, they may also not be indicative of an intrusion and could just be caused by normal user activity. As such, a POSITA would have understood that some of these factors are more likely to indicate an intrusion than others and a combination of these factors may be more likely to indicate an intrusion, and a POSITA would understand that these are the types of rules that a data mining algorithm would produce when producing "rules for system call sequences, and statistics methods for other logs." EX-1005, 14; EX-1003, ¶96.

It therefore would have been obvious to a POSITA that these different factors could be weighted differently and combined together in an equation. EX-1003, ¶97. As such, a POSITA would have been motivated to weigh each factor differently in the rules/heuristics calculations. *Id*. As such, to the extent Li does not explicitly use the words "weighted factors," it would have been obvious to a POSITA to modify

the rules in Li to use weighted factors, and then compare the result to the disclosed threshold (e.g., 48% vs. 50%). *Id*.

**[1D]: identifying, based upon the API call activity, a suspected pestware object on the computer;**

Li discloses [1D]. EX-1003, ¶98.

As discussed *supra* in [1PRE] and [1A], Li discloses monitoring computer activity and identifying activity indicative of potential intrusions, including pestware objects on a computer, based on the computer activity collected in the unified log. Moreover, as discussed *supra* in [1C], Li discloses using different rules and thresholds to analyze the computer activity to determine if a suspected software file is malware. EX-1003, ¶95. More specifically, Li discloses identifying a specific object that is responsible for the intrusion as suspected malware, such as pestware: "[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; *id*., 2 ("At an intrusion, UCLog can be used to ***automatically identify*** the source ***and the execution path of the intrusion***."); EX-1003 ¶99. A POSITA would have understood that the source and the execution path of the intrusion necessarily identified the object residing on the computer that contains the suspected intrusion

(e.g., pestware) and also the network activity that led to the communication of that object. *Id*.

Alternatively, it would have been obvious to a POSITA that, when the source and the execution path was determined, the system in Li could have also identified the specific object associated with that execution path. Furthermore, a POSITA would have been motivated to check the object name to determine if it matched the name of known intrusions. *Id.*, ¶99.

**[1E]: identifying, in response to the identifying the suspected pestware object, a reference to an identity of an externally networked source of the suspected pestware object; and**

Li discloses [1E]. EX-1003, ¶101.

Upon detecting suspected intrusions (like pestware), Li discloses tracing back through the 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."); EX-1003 ¶¶102-103. A POSITA would have understood that the source referenced in Li would have included an externally networked source from which the computer received the file if it was received from an externally networked source. *Id.* Indeed, a POSITA would have understood that intrusions commonly came from the internet,

which consists of externally networked sources like other computers on the internet. *Id.* A POSITA would have further understood that it was at least as likely that the intrusion came from an externally networked source, as opposed to an internal source, such as a USB drive. *Id.* As such, a POSITA would understand "source" in that scenario to refer to an externally networked source from which the object came. *Id.* Given how common it is for intrusions to come from externally networked sources, a POSITA would have understood that Li lends further support by disclosing that a UCLog contains 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." *Id.*, EX-1005, 9; *id.*, 17 (disclosing that the WinDump Log "contains the contents of the UDP and TCP packet headers of all traffic to and from the client machine"). A POSITA would have understood that checking these packet headers would identify externally networked sources of the intrusion. EX-1003 ¶¶102-103.

A POSITA would have understood that the packet headers tracked in a unified log contain the source IP address that indicate the source from which network traffic comes. *Id.*, ¶104. It therefore would have been obvious to a POSITA to check the

source IP address to see from where the malware came to identify a potentially malicious internet source. *Id*.

Li in view of Hartrell also discloses [1E]. *Id.*, ¶105. It would have been obvious to modify Li based on the teachings of Hartrell for the reasons explained above. Like 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; EX-1003, ¶105. Hartrell discloses checking its records to identify the externally networked source (e.g., website) from which malware (like spyware) came: "[T]he 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.'" EX-1006, 3:49-53; *id*., 10:44-50 ("The 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."); EX-1003, ¶105.

**[1F] reporting the identity of the externally networked source to an externally networked pestware research entity, wherein the identity of the externally networked source is selected from a group consisting of an I.P. address, a URL, an email client and a program.**

Li discloses [1F]. EX-1003, ¶106.

Li and Hartrell each disclose sending source information to an administrator, who would receive that information on an externally networked pestware research entity. Li states: "Moreover, it 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 states that the user interface of an IDS "enables an administrator to view the output from the system." *Id.*, 5, 13. If the administrator's user interface is on a separate system, it would be externally networked. EX-1003, ¶107. Li states that "[a]nother solution is running the activity database on a dedicated server." EX-1005, 14. A POSITA would understand that, in that case, the administrator would be on an externally networked research entity. EX-1003, ¶107.

Li in view of Hartrell also discloses [1F]. *Id*., ¶¶107-110. Hartrell discloses: "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." EX-1006. Again, a POSITA would recognize that the "system operator" would be on an externally networked research entity. EX-1003, ¶108.

Moreover, 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.)." EX-1006, 10:25-28. Hartrell also describes providing a snapshot of "local system and network activity to a centralized data store." Hartrell explains that this includes, *intra alia*, "the 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." EX-1006, 4:6-16; EX-1003, ¶109. The centralized data store then makes use of the website/IP address of the externally networked source to determine whether the externally network source is a source of pestware: "[T]he 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***.'" EX-1006, 3:49-53; *id*., 10:44-50 ("The 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.").

A POSITA would therefore understand that the centralized data store described in Hartrell is an externally networked pestware research entity that determines whether the externally networked source is a source of pestware. EX-1003, ¶110. Moreover, Hartrell explicitly discloses sending the externally

networked source information to this centralized data store so that it can make correlations between intrusions on different computers and determine if that source is malicious (*i.e.*, is a source of pestware). EX-1006, 3:38-53, 10:23-50.

**[1G] wherein the identity of the externally networked source is selected from a group consisting of an I.P. address, a URL, an email client and a program.**

As in [1E] and [1F], the externally networked source identified in Li and Hartrell is identified either by an IP address (as disclosed in both Li and Hartrell) or a URL (as disclosed in Hartrell). EX-1005, 9, 17; EX-1006, 4:1-16; EX-1003, ¶¶103-105, 109. It therefore would have been obvious that the externally networked source is identified by an IP address and/or a URL.

Alternatively, it would have been obvious to a POSITA to use an IP address or URL because a POSITA would have understood that these were the two most common ways to refer to networked computers. EX-1003, ¶113.

**b) Claim 2**

**[2P]: The method of claim 1,**

*See supra* Claim 1.

**[2A]: wherein the identifying the suspected pestware object includes accessing an activity log that includes information that relates the activity to the suspected pestware object.**

As in [1A], Li's UCLog includes information related to computer activity, including of a suspected pestware object. EX-1005, 9-11. A POSITA would have understood that activities related to anomalous behavior, for example, would include activity related to suspected pestware. Li discloses tracing the log back to identify the source and execution path of the anomalous behavior as in [1C] and [1D]. EX-1003, ¶XX. If the activity log did not have information related to the activity of the pestware object, Li would not have been able to detect anomalies or the objects, or trace the source. EX-1003, ¶116.

**c) Claim 3**

**[3P]: The method of claim 1,**

*See supra* Claim 1.

**[3A]: wherein the identifying a reference includes accessing at least a portion of a recorded history of externally networked sources.**

Li and Hartrell teach [3A] for the same reasons as [1E]. EX-1003 ¶118.

As in [1E], Li discloses identifying a "source," which a POSITA would have understood to be the externally networked source in the UCLog, meaning that the externally networked source must be identified in the recorded history. EX-1005,

13, 2; EX-1003 ¶120. A POSITA would have understood that the packet headers tracked in UCLog contain the source IP address that indicate the source from which network traffic comes. *Id*. It therefore would have been obvious to a POSITA to check the source IP address to see from where the malware came to identify a potentially malicious internet source. *Id*.

To the extent [3A] would not have been obvious over Li alone, it would have been obvious to combine Li with Hartrell for the reasons explained with [1E]. *Id.*, ¶121. Like 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, 3:49-53, 10:44-50; EX-1003, ¶121.

**d) Claim 4**

**[4P]: The method of claim 3,**

*See supra* Claim 3.

**[4A]: 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.**

In the patent, the "file storage device 218" includes a "browser cache 242" (EX-1001, 6:20-24), which "includes files, cookies, and other objects cached in

connection with use of a browser of the protected computer." *Id*., 6:28-34. Li and Hartrell both describe using recorded history from the file system. Li discloses a "File-System Logger," that can be used to "detect changes to significant blocks." EX-1005, 10. A POSITA would understand that a File-System Logger would log recorded history from a browser cache, which are files stored in the file system. A POSITA would understand that logged recorded history in the browser cache would include information about files downloaded to the computer and a source of each of the files. EX-1003, ¶124.

It also would have been obvious to a POSITA to use an "Application-Specific Logger" as described in Li for a browser application. EX-1005, 10. A POSITA would understand that an Application-Specific Logger for a browser would include information from the browser cache including information about files downloaded to the computer and a source of each of the files. EX-1003, ¶125.

In addition, Hartrell discloses using a "snapshot" of the local system and network activity that includes "web file transfer" activity (EX-1006, 4:37-39) and other sources. *Id.*, 10:23-50, 5:6-12. A POSITA would have understood that web file transfer activity in the snapshot would have included information residing in the browser cache, which includes information about recently downloaded files and the

source of those files. EX-1003, ¶126. And it would have been obvious to a POSITA that Hartrell's snapshot information, including browser cache information, could have been included in the UCLog in Li. *Id*. A POSITA would have recognized that the browser cache would have relevant web file transfer information and so would have been motivated to include it as part of UCLog. EX-1005, 1-3; EX-1003, ¶126.

**e) Claim 5**

**[5P]: A system for identifying a source of activity on a computer that is indicative of pestware including:**

To the extent the preamble is a limitation of the claim, Li and Hartrell teach [5P] for the same reasons as [1P]. EX-1003 ¶¶128-129. Li and Hartrell further teach a ***system*** for performing the method set forth in claim 1. EX-1005, 1-2 (describing a secure logging ***system***); EX-1006, Abstract (describing a malware analysis ***system***).

**[5A]: a kernel-level monitor configured to monitor API call activity on the computer and to store information related to the API call activity in a log;**

Li and Hartrell teach [5A] for the same reasons as [1A]. EX-1003 ¶¶130-131. 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 understand that the kernel API logger and associated monitor in Li is kernel-level

monitor that stores a history of at least a portion of the API calls in the UCLog, which is an activity log. EX-1003 ¶131. As with [1A], a POSITA would have understood or it would have been obvious to a POSITA that a kernel API logger would include a kernel-level monitor. *See* [1A]; EX-1003 ¶131.

**[5B]: a heuristics module configured to analyze the API call activity to determine whether one or more weighted factors associated with the API call activity exceeds a threshold;**

Li and Hartrell teach [5B] for the same reasons as [1C] and [1D]. EX-1003 ¶¶132-133. As in [1C] and [1D], Li discloses using heuristics (i.e., rules) to identify activity indicative of an intrusion, including pestware, based upon weighted factors and a threshold. A POSITA would have understood that the component used to make predictions as to whether activity is an intrusion is the claimed ***heuristics module***. *Id*. ¶133. At minimum, a POSITA would have found it obvious to implement the predictions based on heuristics and thresholds in a separate module, which could be called the heuristics module. *Id*.

**[5C]: a research portion configured to identify, in response to a prompt from the heuristics module, a suspected pestware object on the computer; and**

Li and Hartrell teach [5C] for the same reasons as [1E]. EX-1003 ¶¶135-136. As in [1E], 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 system from Li that traced back through the UCLog is ***the research portion*** that performs the other requirements in [6C]. EX-1003 ¶137 At minimum, it would have been obvious to a POSITA that the code for tracing back through the UCLog to identify the source of the intrusion could have been separated into a ***research portion***. *Id*.

Furthermore, it would have been obvious to POSITA that the tracing back described in Li is performed ***in response to a prompt from the heuristic module*** described in [5B] because the heuristic model identifies a suspected intrusion and this tracing back would be done in response to such an identification. *Id.*, ¶138. A POSITA therefore would have found it obvious that the research portion checks for the source of the intrusion in response to a prompt from the heuristics module identifying a suspected intrusion. *Id*. Further, the recorded information in UCLog would include information ***on the computer***. *Id*. Li describes distributed loggers and loggers operating on the same computer, and so the location of access would be a design choice. *Id*.

To the extent [5C] would not have been obvious over Li alone, it would have been obvious to combine Li with Hartrell for the reasons explained in [1D]. *Id.*, ¶139. Hartrell discloses a ***categorization component*** that will determine whether a file is

malware, like spyware or pestware, an then determine additional information about the file, such as its externally networked source. EX-1006, 6:66-7:15, 8:10-9:28, Figs. 3, 5, 6. A POSITA would have therefore understood that the portion of the categorization component that determines the additional information about the file, such as the externally networked source, is ***the research portion*** that performs the other requirements in [5C]. EX-1003, ¶139. At minimum, it would have been obvious to a POSITA that portion of the categorization component that determines the additional information about the file could have been separated into a research portion. *Id*.

Furthermore, it would have been obvious to POSITA that the determination of additional information in Hartrell is performed ***in response to*** a prompt from the portion of the categorization component that determines a file is suspected malware because the additional information is only determined in response to such an identification of a file as malware. *Id.*, ¶140. This is depicted in Figure 2 of Hartrell, which shows that, once a notification of suspected malware infection is received **206**, then it will generate a post infection snapshot **210** and send it for further processing and/or analysis **212**. EX-1006, FIG2, 6:32-52. A POSITA therefore would have at least found it obvious that the research portion checks for the source

in response to a prompt from another part of the categorization component that identifies a file as potential malware. EX-1003 ¶140.

**[5D]: a reporting portion configured to generate a report including a reference to an identity of an externally networked source of the suspected pestware object and to report the identity of the externally networked source to an externally networked pestware research entity, wherein**

Li and Hartrell teach [5D] for the same reasons as [1F]. EX-1003 ¶¶141-142.

Furthermore, Hartrell discloses 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 recognize that the disclosed snapshot is ***a generated report that identifies the externally networked source of the file***. EX-1003 ¶143. That report is then sent to the centralized data store (externally networked pestware research entity), which then compares the snapshot against reports from other computers to make a determination about whether the networked source is a source of malware, like pestware. *Id*. A POSITA would have found it obvious that the portion that generates this snapshot for the centralized data store could be separated into a ***reporting portion*** of the code. *Id.* As in [1E], Li in combination with Hartrell therefore renders this limitation obvious. *Id*.

**[5E] the kernel-level monitor is configured to store information about a relationship between at least one API call of the API call activity and a file.**

Li and Hartrell teach [5E] for the same reasons as [1B] and [1D]. EX-1003 ¶¶144-145.

As in [1D], Li discloses identifying a specific object that is responsible for the intrusion as suspected malware, like pestware. EX-1005, 13, 2; EX-1003 ¶146. A POSITA would have understood that the execution path of the intrusion necessarily identified the object residing on the computer that contains the suspected intrusion (e.g., pestware). *Id*. A POSITA would have understood that, to identify the object on the computer, UCLog necessarily would have included information about the relationship between the API calls and a specific file or object on the computer to make trace the API calls back to the specific file or object. *Id*. It would have been very common to include relationships between API calls and specific file or objects in a log at the time. *Id*. Alternatively, it would have been obvious to a POSITA to include information about the relationship between the API calls and a specific file or object on the computer so that the trace between the API calls back to the specific file or object was easy to determine. *Id*.

**f) Claim 6**

**[6P]: The system of claim 5,**

*See supra* Claim 5.

**[6A]: wherein the information comprises an identity of at least one process that made at least on API call in the log.**

Li and Hartrell teach [6A] for the same reasons as [1A] and [1B]. EX-1003 ¶¶148-149. It would have been obvious to a POSITA that storing the API calls in the log includes the identity of the process that made those API calls. *Id*., ¶149.

**g) Claim 7**

**[7P]: The system of claim 5,**

*See supra* Claim 5.

**[7A]: wherein the heuristics module is configured to receive information about the API call activity from the kernel-level monitor and to determine whether the API call activity is indicative of pestware.**

Li and Hartrell teach [7A] for the same reasons as [5B] and [5C]. EX-1003 ¶¶151-152.

It would have been obvious to a POSITA that the heuristics module receives API call activity information from the kernel-level monitor because the heuristics module needs the API call activity information, which is monitored by the kernel-

level monitor as described in [5B], to make a determination about whether the API call is indicative of pestware as in [5C]. *Id.*, ¶152.

**h) Claim 8**

**[8P]: The system of claim 5,**

*See supra* Claim 5.

**[8A]: wherein the kernel-level monitor is configured to intercept at least one API call.**

Li and Hartrell teach [8A] for the same reasons as [5A]. EX-1003 ¶154. 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 understand that the kernel API logger is an activity monitor that stores a history of at least a portion of the API calls in the UCLog, which is an activity log. EX-1003 ¶155. And as with [1A], a POSITA would have understood or it would have been obvious to a POSITA that the kernel API logger included a kernel-mode driver. EX-1003 ¶155. Furthermore, given that the purpose of the kernel API logger is to monitor or log API calls to the kernel, it would have been obvious to a POSITA that the kernel-mode driver should be adapted to ***intercept*** the API calls to log them. *Id*.

#### i) Claim 9

**[9P]: The system of claim 5,**

*See supra* Claim 5.

**[9A]: wherein the identity of the externally networked source is selected from the group consisting of an I.P. address, a URL, an email client and a program name.**

Li and Hartrell teach [9A] for the same reasons as [1G]. EX-1003 ¶157.

#### j) Claim 10

**[10P]: The system of claim 5,**

*See supra* Claim 5.

**[10A]: wherein the research portion is configured to access at least a portion of a recorded history of externally networked sources.**

Li and Hartrell teach [10A] for the same reasons as [3A]. EX-1003 ¶159.

#### k) Claim 11

**[11P]: The system of claim 10,**

*See supra* Claim 10.

**[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 file monitoring software logs.**

Li and Hartrell teach [11A] for the same reasons as [4A]. EX-1003 ¶161.

### l) Claim 12

**[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:**

To the extent the preamble is a limitation of the claim, Li and Hartrell, teaches [12P] for the same reason as [1P]. EX-1003 ¶¶162-163.

Li and Hartrell both disclose implementing the process described in [1P] using non-transitory computer-readable medium. EX-1005, 3 (explaining that UCLog system was implemented in software); EX-1006, Abstract (same); EX-1003 ¶164.

**[12A]: monitoring, using a kernel-mode driver, API call activity on the computer;**

Li and Hartrell teach [12A] for the same reasons as [1A]. EX 1003 ¶165.

**[12B]: storing information related to the API call activity in a log;**

Li and Hartrell teach [12B] for the same reasons as [1B]. EX 1003 ¶166.

**[12C]: analyzing, heuristically, the API call activity to determine whether one or more weighted factors associated with the API call activity exceeds a threshold;**

Li and Hartrell teach [12C] for the same reasons as [1C]. EX 1003 ¶167.

**[12D]: identifying, based upon the API call activity, a suspected pestware object on the computer;**

Li and Hartrell teach [12D] for the same reasons as [1D]. EX 1003 ¶168.

**[12E]: identifying, in response to the identifying the suspected pestware object, a reference to an identity of an externally networked source of the suspected pestware object; and**

Li and Hartrell teach [12E] for the same reasons as [1E]. EX 1003 ¶169.

**[12F]: reporting the identity of the externally networked source to an externally networked pestware research entity, wherein**

Li and Hartrell teach [12F] for the same reasons as [1F]. EX 1003 ¶170.

**[12G]: the identity of the externally networked source is selected by an identifier selected from a group consisting of an I.P. address, a URL, an email client and a program.**

Li and Hartrell teach [12G] for the same reasons as [1G]. EX 1003 ¶171.

**m) Claim 13**

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

*See supra* Claim 12.

**[13A]: wherein the instructions for identifying the suspected pestware object include instructions for accessing an activity log that includes information that relates the activity to a suspected pestware object.**

Li and Hartrell teach [13A] for the same reasons as [2A]. EX 1003 ¶173.

**n) Claim 14**

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

*See supra* Claim 12.

**[14A]: wherein the instructions for identifying a reference include instructions for accessing at least a portion of a recorded history of externally networked sources.**

Li and Hartrell teach [14A] for the same reasons as [3A]. EX 1003 ¶175.

**o) Claim 15**

**[15P]: The non-transitory computer-readable medium of claim 14,**

*See supra* Claim 14.

**[15A]: 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.**

Li and Hartrell teach [15A] for the same reasons as [4A]. EX 1003 ¶177.

**B. <u>Ground 2: Claims 1-15 are obvious under § 103 over Li, Hartrell, and Mandujano.</u>**

To the extent, Li and Hartrell do not render obvious every limitation of claims 1-15, the claims would have been obvious over Li, Hartrell, and Mandujano.

Mandujano was published at least by December 9, 2004. EX-1009, ¶¶39, 44. Mandujano, therefore, qualifies as prior art under 35 U.S.C. § 102(b). Like Li and Hartrell, Mandujano describes a malware detection system. EX-1007, 3-6. Mandujano details a process for identifying potential intrusions using different weights to help determine a weighted "score" associated with a potential intrusion

and then taking different actions depending upon whether the score meets specific thresholds. EX-1007, 106-113. These equations that calculate the weighted scores are rules or heuristics to help identify potential intrusions. EX-1003 ¶179.

### 1. Motivation to Combine and Reasonable Expectation of Success

A POSITA would have been motivated to combine the teachings of Li and Hartrell with Mandujano for multiple reasons, including to produce the obvious, beneficial, and predictable result of using a different scoring system to determine abnormal or potentially malicious behavior. EX-1003 ¶180.

When considering the teachings of Li and Hartrell, a POSITA would also have been motivated to consider the teachings of Mandujano, since all three pertain to the same field of endeavor of malware detection and prevention. EX-1003 ¶181. As stated above, Li describes malware detection system with a unified log to track intrusions back to their source. EX-1005, 13. Along similar lines, Hartrell describes a malware detection system that traces back malware to its source, including sending source information to a centralized server where it can be tracked and aggregated for different computers across a network. EX-1006; *see also* EX-1003 ¶181. Mandujano likewise discloses an intrusion detection system for identifying potential

intrusions, but details a specific scoring method for identifying those potential intrusions. EX-1007, 106-113. For these reasons, Li, Hartrell, and Mandujano are in the same field of endeavor and are analogous to the claimed invention of the '932 Patent.

Moreover, a POSITA would have been motivated to combine the teachings of Li, Hartrell, and Mandujano to obtain predictable and beneficial results. EX-1003 ¶182. As 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, 106-113. A POSITA would have known to modify Li and Hartrell based upon Mandujano because doing so would provide a way for potential intrusions to be scored and handled differently depending upon the likelihood of a serious threat. EX-1003 ¶182.

It would have been obvious to a POSITA that not all potential intrusions include the same level of risk in terms of potential damage or disruption for the

computer. EX-1003 ¶183. As such, a POSITA would have been motivated to provide a score that could identify the potential risk associated with an intrusion and take different actions depending on the score. *Id*. It would have been obvious to a POSITA that it would be beneficial to take action in response to a potential intrusion that is proportional to the potential risk of that intrusion. *Id.* A POSITA therefore would have been motivated to try the scoring system from Mandujano to provide different potential responses to the detected intrusion based upon the risk. *Id*.

Although Mandujano focuses on monitoring local activity and outbound traffic (EX-1007, 3), it also discloses a malware detection system like Li and Hartrell. Furthermore, a POSITA would have recognized that the teachings of weighted factor calculations and threshold comparisons could be used in the Li-Hartrell system described above. EX-1003, ¶ 184. A POSITA would have understood that the rules-based calculation described in Li could have been implemented in a number of ways and would have been motivated to try different rules, including the one disclosed in Mandujano. *Id*. Indeed, 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; EX-1003 ¶184.

It therefore would have been obvious for a POSITA to combine the Li-Hartrell system described above with the scoring system teachings described in Mandujano to provide flexibility of responses based upon the potential threat. EX-1003 ¶185.

### 2. <u>Li over Hartrell and Mandujano render obvious limitations [1C] and [1D]</u>

To the extent Li and Hartrell do not render obvious these limitations, Li, Hartrell, and Mandujano disclose [1C] and [1D]. EX-1003, ¶186. Mandujano discloses using a "score-based system" to determine whether an object is malware. EX-1007, 106. Mandujano details a 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. Mandujano further discloses using the weights $w_i$ to calculate another score π, which again is normalized into the range between 0 and 1:

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

EX-1007, 110. Mandujano discloses combining those two factors σ and π into an integrated score called I:

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

EX-1007, 112.

According to Mandujano, moreover, all those weighted factors are compared against thresholds to determine what action to take:

**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.**

EX-1007, 114. For example, 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). *Id.*; EX-1003, ¶188. Mandujano also discloses that a single one of those weighted factors may be used in certain applications. EX-1007, 114; EX-1003, ¶188.

It would have been obvious to a POSITA to use the similarity weighted factors (σ, π, and I) with the rules set forth in Li. EX-1003, ¶189. A POSITA would have understood that there are many different factors that may be indicative of an intrusion

like pestware, including abnormal increases in network traffic, number of file input/outputs, and registry modifications. *Id*. It would have been obvious to a POSITA that not all of these factors should be weighted evenly and therefore a POSITA would have been motivated to weigh each factor differently in the rules/heuristics. *Id*. As such, a POSITA would have been motivated to look for ways of weighting all of these factors in an equation, like the similarity weighted factors disclosed in Mandujano. *Id*. It therefore would have been obvious to a POSITA to combine Li and Hartrell with Mandujano for the reasons set forth above.

Furthermore, for [1D], it would have been obvious to a POSITA to use the weighted factors and threshold from Mandujano to help identify suspected pestware activity as set forth above, Li then discloses tracing back the UCLog to identify the suspected pestware object. *See* [1D]; EX-1005, 13, 2; EX-1003 ¶ 190.

Claim 1 and its dependent limitations are therefore rendered obvious over Li, Hartrell, and Mandujano. EX-1003 ¶ 191.

#### 3. <u>Li over Hartrell and Mandujano render obvious limitations [5B]</u>

To the extent Li and Hartrell do not render obvious this limitation, Li, Hartrell, and Mandujano teach [6B] for the same reasons as [1C] and [1D]. EX-1003 ¶192.

Furthermore, as in [1C] and [1D], Li, Hartrell, and Mandujano disclose using rules/heuristics to identify activity indicative of an intrusion, including pestware, based upon weighted factors and a threshold. *Id.* A POSITA would have understood that the component used to make predictions as to whether activity is an intrusion is the claimed ***heuristics model***, including the weighted factor calculations and thresholds from Mandujano. *Id*. At minimum, a POSITA would have found it obvious to implement the predictions (including the calculations from Mandujano) based on heuristics and thresholds in a separate module, which could be called the heuristics module. *Id.*

As a result, claim 5 and its dependent limitations are rendered obvious over Li, Hartrell, and Mandujano.

#### 4. Li over Hartrell and Mandujano render obvious limitations [12C] and [12D]

Li, Hartrell, and Mandujano teach [12C] and [12D] for the same reasons as [1C] and [1D]. EX-1003 ¶193.

As a result, claim 12 and its dependent limitations are rendered obvious over Li, Hartrell, and Mandujano.

### C. Ground 3: Claims 1-15 are obvious under §103 over Li and Yadav.

To the extent Patent Owner successfully swears behind Hartrell, Yadav—which was published August 7, 2003 and is therefore prior art §102(b)—has analogous disclosure. EX-1008, cover page.

Yadav describes an intrusion detection system that determines the source of an intrusion. *Id.*, 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, FIG1. Yadav explains that information from multiple sources may be sent to a central security server, which will store information about network sources that will be scrutinized more. *Id.*, 3:1-14, 5:33-41.

#### 1. Motivation to Combine and Reasonable Expectation of Success

A POSITA would have been motivated to combine the teachings of Li and Yadav for multiple reasons, including to produce the obvious, beneficial, and predictable result of facilitating the broad-scale implementation of Li, including by consolidating information of potential threats across multiple computers in a network. EX-1003 ¶196.

When considering Li, a POSITA would also have been motivated to consider the teachings of Yadav, since both pertain to the same field of intrusion detection and prevention. *Id.*, ¶197. As stated above, Li describes an intrusion detection system with a unified log to track intrusions back to their source. EX-1005, 13. Similarly, Yadav describes a malware detection system that traces malware to its source, including sending source information to a central security server where it can be tracked and aggregated for different computers across a network. EX-1008; *see also* EX-1003 ¶197. Li and Yadav are therefore in the same field and are analogous to the claimed invention of the '243 Patent.[3]

Moreover, a POSITA would have been motivated to combine the teachings of Li and Yadav to obtain predictable, beneficial results. *Id.*, ¶198. As explained, Li describes creating a unified log of events on a computer. EX-1005. Similarly, Yadav describes combining information from multiple computers in a central server so as to make malware determinations with information from multiple computers. EX-1008, 3:1-14, 5:33-41. A POSITA would have known to modify Li over Yadav

[3] Although Yadav discloses some functionality as part of a firewall, it also explains that this functionality may be integrated into the monitored nodes, like Li. EX-1008, 3:15-21.

because doing so would aggregate the log information, including information about the source of pestware, within the central server described in Yadav. EX-1003 ¶198. It would have been obvious to a POSITA that combining information from multiple computers in a central security server would have allowed the system to make correlations between pestware on different computers and make determinations about whether a source is malicious based upon information from multiple computers. *Id*. A POSITA would have understood that if pestware infected multiple computers from the same source it is more likely a malicious source than if only a single computer was infected and therefore would reduce the likelihood of incorrectly identifying a source as malicious (*i.e.*, false positive). *Id*.

Furthermore, it would have been obvious for a POSITA to try to combine Li's UCLog with the central server in Yadav because it was well known in the art that centralizing logs in a common data store have the benefit of aggregating information from multiple sources and can be used to determine information about the entire network, as opposed to a single computer in the network. EX-1003 ¶199.

### 2. <u>Li over Yadav renders obvious Claims 1-15</u>

As described above, Li and Hartrell render obvious the Challenged Claims. Here, Petitioner only addresses limitations where Yadav would replace Hartrell in a

similar combination with Li. The same analysis of Li applies to these limitations and the other limitations. Section IX.A; EX-1003 ¶200.

**[1P]**

It would have been obvious to combine Li with Yadav as described above, as Yadav also discloses that intrusions include "attempts to gain unauthorized access to data …." EX-1008, 1:45-46. These attacks that attempt to gain access to data falls within the meaning of pestware described above. *Id*.; EX-1003, ¶201.

**[1E]**

It would have been obvious to combine Li with Yadav as described above because Yadav discloses "[w]hen an intrusion prelude is detected, a source of the intrusion prelude is identified (125). For example, a source IP addresses may be extracted from a packet that is part of the intrusion prelude...." EX-1008, 4:31-41; EX-1003, ¶202. Yadav therefore discloses identifying the externally networked source (e.g., the IP address) from which intrusion came. EX-1008, 4:31-41, FIG1 (annotated); EX-1003, ¶202.

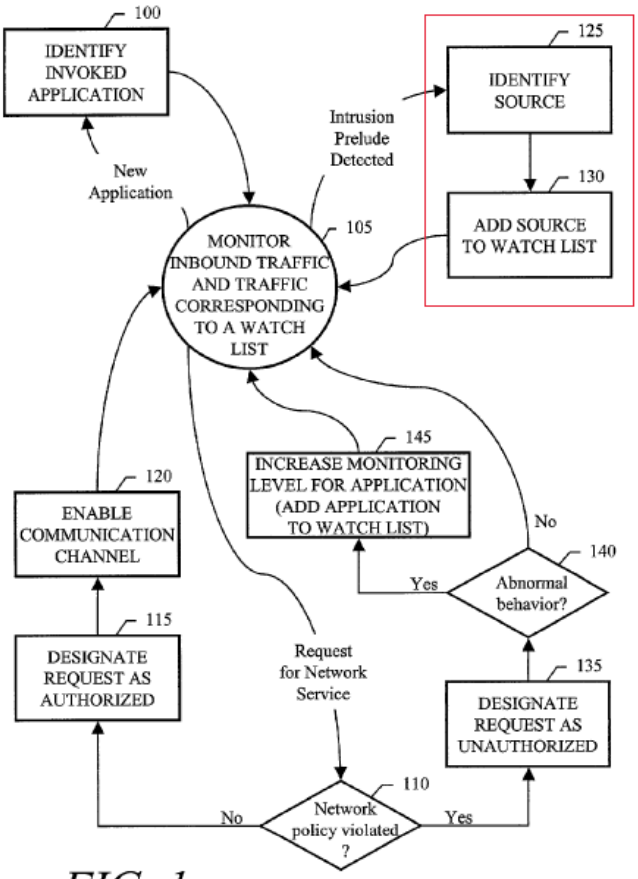


*FIG. 1*

**[1F]**

As in [1E], Li and Yadav render this limitation obvious. EX-1003 ¶203. For example, Yadav discloses, "[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. A POSITA would have understood that the information reported to the central server described in Yadav would have

included the information about the intrusion detected by the system, including information about the source of the intrusion as described for [1D]. EX-1008, 4:31-41, FIG1; EX-1003, ¶204.

A POSITA would have found it obvious and would have been motivated to try to compare the source of intrusions detected by various computers in the network at the central security server to check for common sources of the intrusion. EX-1003, ¶205. A POSITA would understand that the central server described in Yadav is an externally networked pestware research entity that determines whether the source is a source of pestware. *Id*.

Furthermore, to the extent "externally networked pestware research entity" is an administrator, a POSITA would have understood that the administrator could use the central server in Yadav to identify common sources of intrusions as described above. EX-1003, ¶206.

**[1G]**

As in [1E] and [1F], the externally networked source in Li and Yadav is identified by an IP address. EX-1005, 9, 17; EX-1008, 4:31-41, FIG1; EX-1003, ¶207. It therefore would have been obvious that the externally networked source is identified by an IP address and/or a URL. *Id*. Alternatively, it would have been

obvious to a POSITA to use an IP address or URL because a POSITA would have understood that these were the two most common ways to refer to networked computers. *Id*.

**[3A]**

It would have been obvious to combine Li with Yadav as above because Yadav discloses "[w]hen an intrusion prelude is detected, a source of the intrusion prelude is identified (125). EX-1003 ¶208. For example, ***a source IP addresses may be extracted from a packet*** that is part of the intrusion prelude…." EX-1008, 4:31-41; EX-1003, ¶208. A POSITA would have understood that the source IP address could have been extracted from the browser cache that includes information about recently downloaded files and the source of those files. EX-1003, ¶208. It would have been obvious to a POSITA that the information disclosed in Yadav, like the source IP address from the browser cache, could have been included in the UCLog in Li. EX-1003, ¶208. Li discloses that correlating recorded information in UCLog is more effective compared to separate logs and a POSITA would have recognized that the browser cache could have relevant information about recent network activity and would have been motivated to include it as part of UCLog. EX-1005, 1-3; EX-1003, ¶208.

**[4A]**

It would have been obvious to combine Li with Yadav for the reasons described above. EX-1003 ¶209. Yadav discloses "[w]hen an intrusion prelude is detected, a source of the intrusion prelude is identified (125). For example, ***a source IP addresses 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; EX-1003, ¶¶209-210. A POSITA would have understood that the source IP address could have been extracted from the browser cache that includes information about recently downloaded files and the source of those files. EX-1003, ¶210. It would have been obvious to a POSITA that the information disclosed in Yadav, like the source IP address from the browser cache, could have been included in the UCLog in Li. *Id*. Indeed, Li discloses that correlating recorded information in a unified log is more effective in identifying intrusions instead of having separate logs and a POSITA would have recognized that the browser cache could have relevant

information about recent network activity and would have been motivated to include it as part of UCLog. EX-1005, 1-3; EX-1003, ¶210.

**[5P]**

Li and Yadav teach [5P] for the same reasons as [1P]. EX-1003 ¶211. Li and Yadav further teach a ***system*** for performing the method set forth in claim 1. EX-1005, 1-2 (describing a ***system***); EX-1008, Abstract (same).

**[5C]**

It would have been obvious to combine Li with Yadav as in [1E]. Li discloses determining whether there was an intrusion and then determine additional information about the intrusion, such as its externally networked source. EX-1008, 4:31-41; EX-1003, ¶212. A POSITA would have therefore understood that the portion of the system that determines the additional information about the intrusion, such as the externally networked source, is ***the research portion*** that performs the other requirements in [6C]. EX-1003 ¶212. At minimum, it would have been obvious to a POSITA that portion of the system that determines the additional information about the intrusion could have been separated into a research portion. *Id*.

Furthermore, it would have been obvious to POSITA that the determination of additional information in Yadav is performed ***in response to*** a prompt from the portion of the system that determines if a file is a potential intrusion because the additional information is only determined in response to such an identification of an intrusion. *Id.*, ¶213. This is depicted in Figure 1 of Yadav, which shows that, once an intrusion prelude is detected, it will then seek to identify the source. EX-1008, FIG1, 4:31-41. A POSITA therefore would have at least found it obvious that the research portion checks for the source in response to a prompt from another part of the system that identifies a potential intrusion. EX-1003 ¶213.

According to Yadav, moreover, the system will monitor network traffic to determine when there is a potential intrusion based upon traffic flow and port scanning or other rules. EX-1008, 4:18-30. It would have been obvious to a POSITA that the set of network event events (***first set of recorded information***) would be accessed by the system to determine if there is a potential intrusion and so categorize it. EX-1003 ¶213. It likewise would have been obvious to a POSITA that, when determining additional information about the suspected intrusion, the system would access a ***second set of recorded information***, the "network events," which would have additional information, like the externally networked source. *Id.*

**[5D]**

Li and Yadav teach [6D] for the same reasons as [1E]. EX-1003 ¶214.

Furthermore, a POSITA would have understood that, when the system reports information to the central security server, it must generate a report with the relevant information, including at least the source of the intrusion. *Id.*, ¶215. That report is then sent to the central server (externally networked pestware research entity), which then compares the information against reports from other computers to make a determination about whether the networked source is a source of an intrusion, like pestware. *Id*. A POSITA would have found it obvious that the portion that generates this report for the central server could be separated into a ***reporting portion*** of the code. As in [1D], Li and Yadav therefore render this limitation obvious. *Id*.

**[12P]**

Li and Yadav teach [12P] for the same reasons as [1P]. EX-1003 ¶¶216-217. Li and Yadav both disclose implementing the process described in [1P] using non-transitory computer-readable medium. EX-1005, 3 (implementing the system in software); EX-1008, 9:60-65 (disclosing use of memory and other storage).

### D. <u>Grounds 4: Claims 1-15 are obvious under §103 over Li, Yadav, and Mandujano.</u>

The claims would have been obvious over Li, Yadav, and Mandujano.

### 1. Motivation to Combine and Reasonable Expectation of Success

A POSITA would have been motivated to combine the teachings of Li and Yadav with Mandujano for the same reasons as Li, Hartrell, and Mandujano in Section **Error! Reference source not found.**. EX-1003 ¶219. There would not have been any differences in the motivation between Li as modified by Hartrell and Li as modified by Yadav. *Id*.

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

Li, Yadav, and Mandujano disclose [1B] and [1C]. EX-1003, ¶220. Mandujano discloses using a "score-based system" to determine whether an object is malware as described in section **Error! Reference source not found.**, *supra*. EX-1007, 106; EX-1003 ¶220. It would have been obvious to combine Li-Yadav and Mandujano for the reasons set forth above and as described in section **Error! Reference source not found.**, *supra*. EX-1003 ¶220. As a result, claim 1 and its dependent limitations are rendered obvious over Li, Yadav, and Mandujano.

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

Li, Yadav, and Mandujano teach [6B] for the same reasons as [1B] and [1C]. EX-1003 ¶221. Furthermore, as in [1B] and [1C], Li, Yadav, and Mandujano

disclose using rules/heuristics to identify activity indicative of an intrusion, including pestware, based upon weighted factors and a threshold. It would have been obvious to a POSITA for the reasons descried in section **Error! Reference source not found.**, *supra*. EX-1003 ¶221. As a result, 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]

Li, Yadav, and Mandujano teach [12B] and [12C] for the same reasons as [1B] and [1C]. EX-1003 ¶222. As a result, claim 12 and its dependent limitations are rendered obvious over Li, Yadav, and Mandujano.

## X. PTAB DISCRETION SHOULD NOT PRECLUDE INSTITUTION

### A. PTAB should not exercise its discretion to deny institution under *Fintiv*.

Consistent with congressional intent and the goals of *NHK/Finitiv*, Petitioners took all possible steps to promote the Board's efficiency and fairness objectives. Petitioners initiated this petition with diligence (approximately six months after first receiving notice that the '932 patent would be asserted against Sophos, less than six months after receiving infringement contentions), filed a single, focused petition, and served a stipulation (EX-1016) identical to one the Board previously found

mitigated concerns of duplicative efforts between the district court and the Board and potentially conflicting decisions. *Sand Revolution II, LLC v. Continental Intermodal Grp.*, IPR2019-01393, Paper 24 (June 16, 2020). These facts, along with the merits of Grounds 1-3, strongly favor institution.

### 1. Factor 1: Whether Institution Will Increase the Likelihood of a Stay in the District Court

Institution will enable the Board to resolve the issue of validity, and a finding of invalidity will relieve the District Court of the need to thereafter continue with the companion litigation. The District Court has made clear in prior cases that a motion to stay prior to institution of an IPR would be premature, so Petitioners have not yet requested a stay. It is unclear how the District Court would rule on a motion to stay after institution. Indeed, the Board recently "decline[d] to speculate on the likelihood of Judge Albright entering a stay after institution" and thus found Factor 1 neutral. *Western Digital Corp. v. Kuster*, IPR2020-01391, Paper 10 at 9 (Feb. 16, 2021); *see also Volkswagen Grp. of Am., Inc. v. Arigna Tech. Ltd.*, IPR2021-01321, Paper 10 at 7 (Feb. 15, 2022) (declining to speculate about the likelihood of a stay); *VMware Inc. v. Intellectual Ventures II LLC*, IPR2020-00859, Paper 13 at 12 (Nov. 5, 2020) (informative); *Apple Inc. v. Fintiv, Inc.*, IPR 2020-00019, Paper 15 at 12

(May 13, 2020) (declining to speculate regarding stay motions). Thus, this factor is at worst neutral.

### 2. **Factor 2: District Court Schedule**

The District Court schedule weighs in favor of institution. Pursuant to the District Court's amended scheduling order on March 29, 2023 (Dkt. No. 252), the first trial in this case will not begin until August 19, 2024. Because there are multiple defendants and counterclaims, and based upon the fact that the '932 patent is in the third set of patents asserted by Patent Owner against Petitioner, it is unlikely that trial for '932 Patent would begin on that date. Based on an 18-month IPR schedule, a Final Written Decision ("FWD") arising from this petition would issue around October 2024.

Even if it were the case that a FWD would be likely to issue before trial began, uncertainty about the trial date and the high likelihood of further delay weigh against discretionary denial. In general, District Court patent-validity litigation schedules are uncertain. Indeed, the Board has held that this factor was "neutral" even in cases where the projected trial date was close to the Board's statutory final-decision deadline because it has recognized that projected trial dates are uncertain, especially when projected in the early stages of litigation. In *Cizion, LLC v. Kerr Machine Co.*,

for instance, the District Court trial was set "three months prior to [the Board's] (anticipated) deadline for a final written decision." PGR2020-00065, Paper 10 at 26 (Dec. 3, 2020). The Board explained that "[a]lthough the current schedule [in *Cizion*] indicates that trial will commence a few months prior to the statutory due date to issue a final written decision in this proceeding, evidence in the record cited by the Petitioner does indicate that the actual trial date is uncertain." *Id.*

The *Cizion* Board credited the Petitioner's evidence that "in the Western District of Texas, 70% of trial dates have slipped following PTAB discretionary denials." *Id.* The Board further noted that the evidence included "multiple proceedings with trial dates close to the" same trial date. *Id.*; *see also Micron Tech., Inc. v. Godo Kaisha IP Bridge 1*, IPR2020-01008, Paper 10 at 14 (Dec. 7, 2020) ("Accordingly, even if we consider the Texas court to have set a formal trial date for a few months before the final written decision, due to the uncertainty as to this trial date, this factor is, at most, neutral to whether we should exercise our discretion to deny the Petition."). As in *NHK*, District Court trial dates often shift. *Mylan Pharm. Inc. v. Sanofi-Aventis Deutschland GMBH*, IPR2018-01680, Paper 22, 17 (Apr. 3, 2019). The Western District of Texas is one of the country's busiest patent courts, and trial-date shifting is likely. The general uncertainty of District Court patent-

validity actions, and the high likelihood that the litigation will extend beyond its projections, weighs in favor of institution as well.

Finally, trial may be pushed even further back because this case is especially complex—Patent Owner originally asserted nine patents against five defendants. Those cases were consolidated for pretrial purposes. *Webroot, Inc., et al. v. AO Kaspersky Lab*, No. 6:22-cv-00243-ADA-DTG (W.D. Tex.) (Dkt. No. 49). Then, seven months after the original complaints were filed, Patent Owner moved to assert five more patents against Petitioner and other defendants. In granting Patent Owner's motion to amend, the Court acknowledged that this case is "about as complicated as you're going to get with patent cases," EX-1017, 52:7-8, and the Court said it would be "amenable to adjusting the schedule" by "granting more time to address things," *id.*, 52:22-23. Because this multi-defendant consolidated case is exceptionally complicated, it is unlikely that the District Court will dispose of the dispute over the '932 Patent before a FWD would issue.

In any event, recent Interim Guidance[4] dictates that because scheduled trial dates "are unreliable and often change," a scheduled trial date "is not by itself a good

[4] https://www.uspto.gov/sites/default/files/documents/interim_proc_discretionary_denials_aia_parallel_district_court_litigation_memo_20220621_.pdf

indicator of whether the district court trial will occur before the statutory deadline for a [FWD]." *Samsung Elec.'s Co., Ltd. et all v. Staton Techniya, LLC*, IPR2022-00302, Paper 13, 10 (PTAB July 11, 2022).

Thus this factor weighs strongly against discretionary denial.

### 3. Factor 3: Petitioners' Investment in the IPR Outweighs Forced Investment in Litigation to Date

Petitioners' substantial investment in these IPR proceedings should counterbalance—if not outweigh—the resources invested in the co-pending litigation. It would be unjust to consider resources expended in the District Court (equally by both parties), without considering Petitioners' resources expended to prepare this IPR petition that would be irretrievably lost without consideration on the merits, in addition to the extensive expenses that may be foregone through institution of this petition and that will otherwise certainly follow in co-pending litigation for which significant milestones exist. *See, e.g.*, *Apple v. Seven Networks*, IPR2020-00255, Paper 13 at 12-15 (July 28, 2020) (declining to exercise discretionary denial on petitions filed nine months after the commencement of co-pending litigation where a large number of patents were included in the litigation, and a large number of claims from each patent were challenged in the petitions).

In *Sand Revolution*, even after invalidity contentions and the *Markman* hearing, the Board found that this factor weighed "only marginally, if at all, in favor of exercising discretion." *Sand Revolution*, IPR2019-01393, Paper 24 at 11. Given Petitioners' diligence and significant investment in filing this petition, especially this early in the litigation, this factor should weigh against a discretionary denial.

#### 4. Factor 4: The Petition Raises Unique Issues

Factor 4 strongly supports institution. Consistent with *Fintiv*, Petitioners ask the Board to consider the unique challenges raised in the petition. Petitioners have stipulated that, if the Board institutes the present petition, Petitioners will not assert that the challenged claims are invalid on the instituted grounds in the related litigation, nor any other possible prior art printed publication grounds based on the references in Grounds 1-2. EX-1016. This stipulation is similar to the stipulation in *Sand Revolution* and therefore this factor strongly supports institution. *Sand Revolution*, Paper 24 at 11.

#### 5. Factor 5: Institution Will Provide the Board an Opportunity to Invalidate Claims That Could Be Later Reasserted against Others

In the District Court litigation, as noted above, Patent Owner has asserted 15 patents against five defendants. Of those 15 patents, five are asserted against all five

defendants; five are asserted against four defendants; and the average patent is asserted against 3.6 defendants. (In fact, Patent Owners have asserted the '932 Patent against all other co-defendants). *See Webroot, Inc. et al. v. AO Kaspersky Lab*, Case No. 6:22-CV-00243 (W.D. Tex.)). In other words, Patent Owner has a demonstrated history of asserting claims against multiple defendants, and the Board has an opportunity to invalidate some of those claims here. Factor 5 weighs in favor of institution.

### 6. Factor 6: Other Circumstances Support Institution

As explained above, the merits of the unpatentability grounds are particularly strong, weighing in favor of institution. See *Fintiv* at 14-15. And the effect on "the economy [and] the integrity of the patent system" further supports institution. *PTAB Consolidated Trial Practice Guide* 59 (Nov. 2019). The claims of the '932 Patent are very broad and purport to cover identifying the source from where malware came, which was already in disclosed several years prior to even the earliest priority date of the patent. The Board should consider and invalidate the claims such that they may not be asserted against other entities in the future.

### B. PTAB should not exercise its discretion to deny institution under *Becton* and *Advanced Bionics*.

Furthermore, institution should not be denied under the framework set forth in *Becton, Dickinson & Co. v. B. Braun Melsungen AG*, IPR2017-01586, Paper 8 (Dec. 15, 2017) (precedential as to § III.C.5, first paragraph) and *Advanced Bionics LLC v. MED-EL Elektromedizinische Gerate GmbH*, IPR2019-01469, Paper 6 (PTAB Feb. 13, 2020) (precedential). None of Li, Hartrell, Mandujano, nor Yadav was before the Examiner during prosecution. Therefore, the arguments presented in this Petition are not the same as, or substantially similar to, arguments previously presented to the Office. Thus, the first prong of the *Advanced Bionics* framework is not met. And because the first prong is not met, there is no need to reach the second prong to resolve against discretionary denial under Section 325(d)—though in any event, there are no pending proceedings before the PTAB concerning the '932 Patent, so the second prong is not met either. *Oticon Medical AB v. Cochlear Ltd.*, IPR2019-00975 Paper 15, 20 (PTAB Oct. 16, 2019) (precedential).

## XI. CONCLUSION

Petitioners respectfully request that this petition be granted, that review be instituted, and that the Challenged Claims be found unpatentable and cancelled.

DATED: April 4, 2023 Respectfully Submitted,

By: */s/ Ryan Iwahashi*
Ryan Iwahashi
(Reg. No. 63,378)
Gibson, Dunn & Crutcher LLP
1881 Page Mill Road
Palo Alto, CA 94304-1211
Tel: (650) 849-5367
RIwahashi@gibsondunn.com

## XII. CERTIFICATE OF WORD COUNT

Pursuant to 37 C.F.R. § 42.24, the undersigned attorney for the Petitioners declares that the argument section of this petition (Sections I, III-XI) has a total of 13,999 words, according to the word count tool in Microsoft Word™.

DATED: April 4, 2023

Respectfully Submitted,

By: */s/ Ryan Iwahashi*

Ryan Iwahashi
(Reg. No. 63,378)
Gibson, Dunn & Crutcher LLP
1881 Page Mill Road
Palo Alto, CA 94304-1211
Tel: (650) 849-5367
RIwahashi@gibsondunn.com

## CERTIFICATE OF SERVICE

The undersigned certifies service pursuant to 37 C.F.R. §§ 42.6(e) and 42.105(a), (b) on the Patent Owner via FedEx overnight mail of a copy of this Petition for *Inter Partes* Review and supporting materials at the Patent Owner at the correspondence address of record for the ’932 Patent:

Assignee:
Webroot Inc.
Two Avenue de Lafayette
6th Floor
Boston, Massachusetts 02111

Counsel of Record:

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

DATED: April 4, 2023

By: */s/ Ryan Iwahashi*
Ryan Iwahashi
(Reg. No. 63,378)
Gibson, Dunn & Crutcher LLP
1881 Page Mill Road
Palo Alto, CA 94304-1211
Tel: (650) 849-5367
RIwahashi@gibsondunn.com