

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

TREND MICRO, INC.
Petitioner

v.

WEBROOT, INC.

Case No. IPR2023-01391
Patent No. 8,719,932

**PETITION FOR INTER PARTES REVIEW
OF U.S. PATENT NO. 8,719,932**

Filed on behalf of Trend Micro
By: Robert M. Hansen
Matthew J. Anderson
Scott B. Amankwatia
The Marbury Law Group, PLLC
11800 Sunrise Valley Drive
15th Floor
Reston, VA 20191

Tel: (703) 391-2900
Fax: (703) 391-2901

TABLE OF CONTENTS

I. Mandatory Notices (37 C.F.R. § 42.8(a)(1))	1
II. Grounds for Standing (37 C.F.R. § 42.104(a)).....	3
III. Identification of Challenge (37 C.F.R. § 42.104(b)).....	3
A. Citation of Prior Art.....	3
B. Statutory Grounds for Challenge.....	4
IV. The '932 Patent.....	5
A. Claim of Priority of the '932 patent	5
B. Specification of the '932 Patent	5
C. Summary of the Prosecution History	6
D. Level of Ordinary Skill in the Art	7
E. Claim Construction.....	7
V. Grounds of Rejection.....	8
A. Ground 1: Claims 1-15 are unpatentable under 35 U.S.C. § 103(a) as obvious in view of Abad and Piccard.....	9
1. Claim 1	11
a. A method for identifying an origin of activity on a computer that is indicative of pestware comprising:.....	11
b.monitoring, using a kernel-mode driver, API call activity on the computer;	12
c.storing information related to the API call activity in a log;.....	12
d.analyzing, heuristically, the API call activity to determine whether one or more weighted factors associated with the API call activity exceeds a threshold;	13
e.identifying, based upon the API call activity, a suspected pestware object on the computer;	14

f. 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	15
g. reporting the identity of the externally networked source to an externally networked pestware research entity, ...	16
h. 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. .	16
2. Claim 2	17
The method of claim 1, wherein the identifying the suspected pestware object includes accessing an activity log that includes information that relates the activity to the suspected pestware object.	17
3. Claim 3	18
The method of claim 1, wherein the identifying a reference includes accessing at least a portion of a recorded history of externally networked sources.	18
4. Claim 4	19
The method of claim 3, 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.	19
5. Claim 5	20
a. A system for identifying a source of activity on a computer that is indicative of pestware including:.....	20
b. 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;..	20
c. 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;.....	21

d.a research portion configured to identify, in response to a prompt from the heuristics module, a suspected pestware object on the computer; and	22
e.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, ...	23
f.wherein 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.	24
6. Claim 6	25
The system of claim 5, wherein the information comprises an identity of at least one process that made at least one API call in the log	25
7. Claim 7	26
The system of claim 5, 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.....	26
8. Claim 8	27
The system of claim 5, wherein the kernel-level monitor is configured to intercept at least one API call.....	27
9. Claim 9	28
The system of claim 5, 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.....	28
10. Claim 10	28
The system of claim 5, wherein the research portion is configured to access at least a portion of a recorded history of externally networked sources.....	28
11. Claim 11	30
The system of claim 10, 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.	30
12. Claim 12	31
a.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:.....	31
b.monitoring, using a kernel-mode driver, API call activity on the computer;	31
c.storing information related to the API call activity in a log;.....	32
d.analyzing, heuristically, the API call activity to determine whether one or more weighted factors associated with the API call activity exceeds a threshold;	32
e.identifying, based upon the API call activity, a suspected pestware object on the computer;	32
f.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	32
g.reporting the identity of the externally networked source to an externally networked pestware research entity, wherein.....	32
h.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.	33
13. Claim 13	33
The non-transitory computer-readable medium of claim 12, wherein the instructions for identifying the suspected pestware object include instructions for accessing an activity log that includes information that relates the activity to the suspected pestware object.....	33
14. Claim 14	34

The non-transitory computer-readable medium of claim 12, wherein the instructions for identifying a reference include instructions for accessing at least a portion of a recorded history of externally networked sources.....	34
15. Claim 15	34
The non-transitory computer-readable medium of claim 14, 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.	34
B. Ground 2: Claims 1-15 are unpatentable under 35 U.S.C. § 103 as obvious by Kilpatrick in view of Piccard.	35
1. Claim 1	37
a.A method for identifying an origin of activity on a computer that is indicative of pestware comprising:.....	37
b.monitoring, using a kernel-mode driver, API call activity on the computer;	37
c.storing information related to the API call activity in a log;.....	38
d.analyzing, heuristically, the API call activity to determine whether one or more weighted factors associated with the API call activity exceeds a threshold;	38
e.identifying, based upon the API call activity, a suspected pestware object on the computer;	39
f.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	40
g.reporting the identity of the externally networked source to an externally networked pestware research entity, wherein.....	41
h.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.	42

2. Claim 2	43
The method of claim 1, wherein the identifying the suspected pestware object includes accessing an activity log that includes information that relates the activity to the suspected pestware object.	
3. Claim 3	44
The method of claim 1, wherein the identifying a reference includes accessing at least a portion of a recorded history of externally networked sources.	
4. Claim 4	45
The method of claim 3, 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.	
5. Claim 5	46
a.A system for identifying a source of activity on a computer that is indicative of pestware including:.....	
b.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;..	
c. 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;.....	
d.a research portion configured to identify, in response to a prompt from the heuristics module, a suspected pestware object on the computer; and	
e.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	

f. 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.	50
6. Claim 6	51
The system of claim 5, wherein the information comprises an identity of at least one process that made at least one API call in the log.....	51
7. Claim 7	52
The system of claim 5, 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.....	52
8. Claim 8	53
The system of claim 5, wherein the kernel-level monitor is configured to intercept at least one API call.....	53
9. Claim 9	54
The system of claim 5, 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.....	54
10. Claim 10	55
The system of claim 5, wherein the research portion is configured to access at least a portion of a recorded history of externally networked sources.....	55
11. Claim 11	56
The system of claim 10, 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.	56
12. Claim 12	57

a. 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:.....	57
b.monitoring, using a kernel-mode driver, API call activity on the computer;	57
c.storing information related to the API call activity in a log;.....	58
d.analyzing, heuristically, the API call activity to determine whether one or more weighted factors associated with the API call activity exceeds a threshold;	58
e.identifying, based upon the API call activity, a suspected pestware object on the computer;	58
f.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	58
g.reporting the identity of the externally networked source to an externally networked pestware research entity, ...	58
h.wherein 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.	59
13. Claim 13	60
The non-transitory computer-readable medium of claim 12, wherein the instructions for identifying the suspected pestware object include instructions for accessing an activity log that includes information that relates the activity to the suspected pestware object.....	
14. Claim 14	60
The non-transitory computer-readable medium of claim 12, wherein the instructions for identifying a reference include instructions for accessing at least a portion of a recorded history of externally networked sources.....	
15. Claim 15	61

The non-transitory computer-readable medium of claim 14, 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. 61

VI. NO BASIS FOR DISCRETIONARY DENIAL.....61

VII. CONCLUSION 63

TABLE OF AUTHORITIES

Cases

<i>Advanced Bionics, LLC v. MED-EL Elektromedizinische Gerate GmbH</i> , IPR2019-01469, Paper 6 (Feb. 13, 2020).....	62
<i>Cellco Partnership v. Huawei Device Co.</i> , IPR2020-01117, Paper 10 (Feb. 3, 2021).....	63
<i>General Electric v. Vestas</i> , IPR2018-00928, Paper 9, *16-17 (PTAB Nov. 5, 2018)	8
<i>Graham v. John Deere Co.</i> , 383 U.S. 1 (1966)	9
<i>KSR Int’l Co. v. Teleflex, Inc.</i> , 550 U.S. 398 (2007)	9
<i>Phillips v. AWH Corp.</i> , 415 F.3d 1303 (Fed. Cir. 2005) (en banc)	7
<i>Sotera Wireless, Inc., v. Masimo Corp.</i> , No. IPR2020-01019, Paper 12 at 19 (P.T.A.B. Dec. 1, 2020)	61
<i>Western Digital Corporation v. Spex Technologies, Inc.</i> , IPR2018-00084, Paper 14, *11 (PTAB Apr. 25, 2018)	8

Statutes

35 U.S.C. § 102(b)	3, 4
35 U.S.C. § 102(e)	4
35 U.S.C. § 103	passim
35 U.S.C. § 325(d)	61, 63
35 U.S.C. §§ 314(a)	61

Rules

37 C.F.R. § 42.10(a).....	2
37 C.F.R. § 42.104(a).....	3
37 C.F.R. § 42.8(a)(1).....	1
37 C.F.R. § 42.8(b)(2).....	1
37 C.F.R. § 42.8(b)(3).....	2

EXHIBIT LIST

Exhibit No.	Description
1001	U.S. Patent No. 8,719,932 to Boney.
1002	Prosecution History of '932.
1003	Expert Declaration of Dr. Seth Nielson.
1004	Curriculum Vitae of Dr. Seth Nielson.
1005	Webroot, Inc. and Open Text, Inc. v. Trend Micro Inc., Case No. 6:22-cv-00243-ADA-DTG, Claim Construction Order, Dkt. 391 (W.D. Tex., July 25, 2023).
1006	Cristina Abad, <i>Log Correlation for Intrusion Detection: A Proof of Concept</i> , 19th Annual Computer Security Applications Conference (2003).
1007	U.S. Patent Publication No. 2007/0006310 to Piccard.
1008	U.S. Patent No. 6,735,703 to Kilpatrick <i>et al.</i>
1009	Ed Skoudis, <i>Malware: Fighting Malicious Code</i> , Pearson (Nov. 2003).
1010	Robert Rinnan, <i>Benefits of Centralized Log File Correlation</i> , Gjøvik University College (2005).
1011	Platform SDK: Windows Management Instrumentation, <i>Win32_Process</i> , Win32_Process class [WMI] (archive.org) (Jul. 17, 2004).
1012	Matthew M. Lavy, <i>Windows Management Instrumentation (WMI)</i> , Sams (Oct. 2001).

Exhibit No.	Description
1013	Yariv Kaplan, <i>API Spying Techniques for Windows 9x, NT and 2000</i> , API Spying Techniques for Windows 9x, NT and 2000 (archive.org) (Feb. 10, 2003).
1014	Stephanie Forrest, <i>Computer Immunolgy</i> , <i>Communications of the ACM</i> 40(1), (Oct. 1997).
1015	Declaration of Ingrid Hsieh-Yee, Ph.D.

Trend Micro America, Inc. and Trend Micro, Inc. (collectively “Petitioner”) petitions for *inter partes* review of claims 1-15 of U.S. Patent No. 8,719,932 to Boney, entitled “Backwards researching activity indicative of pestware” (“the ‘932 patent,” Ex. 1001), which according to PTO records, is assigned to Webroot, Inc.

I. Mandatory Notices (37 C.F.R. § 42.8(a)(1))

REAL PARTY IN INTEREST:

The real parties-in-interest are Trend Micro, Inc., Trend Micro America, Inc. and Trend Micro, Incorporated. Trend Micro, Inc. is a wholly owned subsidiary of Trend Micro America, Inc., which is a wholly owned subsidiary of Trend Micro Incorporated, a Japanese Corporation.

RELATED MATTERS:

Pursuant to 37 C.F.R. § 42.8(b)(2), Petitioner identifies the following related matters.

A petition for *inter partes* review is being filed concurrently with respect to U.S. Patent No. 8,726,243, which is the parent application of the ‘932 patent.

The ‘932 patent is also at issue in the following district court litigations:

- *Webroot, Inc. and Open Text, Inc. v. Trend Micro Inc.*, Case No. 6:22-cv-00239 (W.D. Tex.), which was originally filed on March 4, 2022.

- *Webroot, Inc. and Open Text, Inc. v. Sophos LTD.*, Case No. 6:22-cv-00240 (W.D. Tex.), which was originally filed on March 4, 2022.
- *Webroot, Inc. and Open Text, Inc. v. CrowdStrike, Inc. and CrowdStrike Holdings, Inc.*, Case No. 6:22-cv-00241 (W.D. Tex.), which was originally filed on March 4, 2022.
- *Webroot, Inc. and Open Text, Inc. v. AO Kaspersky Lab*, Case No. 6:22-cv-00243 (W.D. Tex.), which was originally filed on March 4, 2022.

LEAD AND BACKUP COUNSEL:

Pursuant to 37 C.F.R. § 42.8(b)(3) and 37 C.F.R. § 42.10(a), Petitioner appoints:

Robert M. Hansen (Reg. No. 43,656) as lead counsel,

Scott B. Amankwatia (Reg. No. 78,226) as back-up counsel, and

Matthew J. Anderson (Reg. No. 78,257) as back-up counsel.

Pursuant to 37 C.F.R. § 42.10(b), a power of attorney is being filed with this designation of counsel.

SERVICE INFORMATION:

Petitioner provides the following service information for designated counsel:

The Marbury Law Group, PLLC
11800 Sunrise Valley Drive
15th Floor
Reston, VA 20191
Tel: (703)-391-2900
Fax: (703)-391-2900

Petitioner consents to electronic service by email to the email addresses:

rhansen@marburylaw.com;

samankwatia@marburylaw.com;

manderson@marburylaw.com; and

pat-docketing@marburylaw.com.

PAYMENT OF FEES

The PTO is authorized to charge any fees due during this proceeding to
Deposit Account No. 18-1579.

II. Grounds for Standing (37 C.F.R. § 42.104(a))

Petitioner certifies that the '932 patent is available for *inter partes* review and that Petitioner is not barred or estopped from requesting an *inter partes* review challenging the patent claims on the grounds identified in this Petition.

III. Identification of Challenge (37 C.F.R. § 42.104(b))

A. Citation of Prior Art

Petitioner cites the following prior art references:

Abad, Cristina. *Log Correlation for Intrusion Detection: A Proof of Concept*, 19th Annual Computer Security Applications Conference (2003), (“Abad,” EX1006) is prior art under pre-AIA § 102(b) because it was published at the latest on January 12, 2004, more than 1 year before the earliest possible priority date of

the '932 patent. EX1015. Abad was not disclosed to or considered by the Examiner who allowed the '932 patent.

U.S. Published Patent Application No. 2007/0006310, (“Piccard,” EX1007) is prior art under pre-AIA § 102(e) because it was filed on June 30, 2005, before the earliest possible priority date of the '932 patent. Piccard was not submitted to or considered by the Examiner who allowed the '932 patent.

U.S. Patent No. 6,735,703, (“Kilpatrick,” EX1008) is prior art under pre-AIA § 102(b) because it was published on May 11, 2004, more than one year before the earliest possible priority date of the '932 patent. Kilpatrick was not submitted to or considered by the Examiner who allowed the '932 patent.

B. Statutory Grounds for Challenge

Petitioner requests review of claims 1-30 on the following grounds:

GROUND 1: Claims 1-15 is unpatentable under pre-AIA 35 U.S.C. § 103(a) as obvious in view of Abad (EX1006) and Piccard (EX1007).

GROUND 2: Claims 1-15 are unpatentable under 35 U.S.C. § 103 as obvious in view of Kilpatrick (EX1008) and Piccard (EX1007).

IV. The '932 Patent

A. Claim of Priority of the '932 patent

The '932 patent, entitled “Backwards Researching Activity Indicative Of Pestware,” issued on 5/6/14, from U.S. Patent Application No. 13/490,294, filed 6/6/12, which is continuation of patent U.S. Patent Application No. 11/408,146, filed 4/20/06. EX1001, Front Cover.

B. Specification of the '932 Patent

The ‘932 patent describes methods for identifying an origin of activity on a computer that is indicative of pestware, systems for identifying a source of activity on a computer that is indicative of pestware, and a non-transitory computer-readable medium including processor-executable instructions for identifying an origin of activity on a computer that is indicative of pestware. EX1001, 10:20-12:31.

Specifically, claims 1-4 are directed to a method for identifying an origin of activity on a computer that is indicative of pestware that includes monitoring API call activity; storing information related to APIC call; analyzing API call; identifying suspected pestware object; and identifying an externally networked source. EX1001, 10:20-39. Dependent claims 2-4 recite further limitations regarding identifying suspected pestware object and a reference. *Id.* at 10:40-52.

Claims 5-11 are directed to a system for identifying a source of activity on a computer that is indicative of pestware that includes a kernel-level monitor, heuristics module, a research portion, and a reporting portion. *Id.* at 10:53-11:26. Dependent claims 6-11 recite further limitations regarding the information, the heuristics module, the kernel-level monitor, the externally networked source, the research portion, and the recorded history. *Id.* at 11:6-26.

Claims 12-15 are directed to the non-transitory computer-readable medium including processor-executable instructions for identifying an origin of activity on a computer that is indicative of pestware. *Id.* at 11:27-12:31. Dependent claims 13-16 recite further limitations regarding the instructions for identifying the suspected pestware object, instructions for identifying a reference, and the recorded history. *Id.* at 12:17-31.

C. Summary of the Prosecution History

Prosecution began with an Examiner initiated interview on 12/12/13. EX1002, p. 21. During the interview, the Examiner indicated that claims 1, 3-6, 8-14, and 16-18 raised a nonstatutory obviousness-type double patenting issue over claims 1-14 of U.S. Patent No. 8,201,243. *Id.* at 22. In response, Applicant filed a terminal disclaimer on 12/12/13. In the Notice of Allowability dated 12/26/13, the Examiner proposed an amendment to the independent claims that included the

limitation: “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.” *Id.* at 22-26.

The Examiner asserted that the proposed limitation was sufficient because the claims are directed to detecting, controlling and/or removing pestware – which would thus include the proposed amended features. *Id.* at 27.

D. Level of Ordinary Skill in the Art

As established by the Declaration of Dr. Seth Nielson dated 9/7/2023 (*See* EX1002, ¶93), a person having ordinary skill in the art (PHOSITA) at the time of the earliest claimed priority date for the '932 patent would have had a bachelor's degree in computer science, or a related field, or an equivalent technical degree or equivalent work experience, and an additional one to two years of education or experience in the field of computer security topics such as malware/exploit detection. EX1003, ¶93. More education can supplement practical experience and vice versa.

E. Claim Construction

In this proceeding, claims are interpreted under the same standard applied by Article III courts (i.e., the *Phillips* standard). 37 C.F.R. §42.100(b); *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc).

In parallel litigation, Webroot argued claim terms in asserted patents should be given their plain and ordinary meanings. Likewise, the claim construction order

in this parallel litigation by the Western District of Texas court construed contested terms in the '244, '243, and '932 patent under their plain and ordinary meaning with the exception of “pestware.” EX1005, p.3. Specifically, the court construed “pestware” to mean “A trojan, spyware, or adware program that collects information about a person or an organization.” *Id.* For purposes of this proceeding only, Petitioner proposes the Board adopt plain and ordinary meaning as proposed by Webroot and adopted by the Western District of Texas court for terms other than “pestware” and adopt the court’s construction of “pestware.” *See Western Digital Corporation v. Spex Technologies, Inc.*, IPR2018-00084, Paper 14, *11 (PTAB Apr. 25, 2018) (finding Petition based on claim constructions urged by Patent Owner satisfies the claim construction requirements and Petitioner is not required to express its subjective agreement regarding correctness of the proffered claim construction or take ownership of the construction); *see also General Electric v. Vestas*, IPR2018-00928, Paper 9, *16-17 (PTAB Nov. 5, 2018).¹

V. Grounds of Rejection

The following discussion and the accompanying evidence demonstrate that there is a reasonable likelihood that Petitioner will prevail with respect to the

¹ Petitioner reserves the right in other proceedings to construe the Challenged Claims and pursue indefiniteness theories.

challenged claims.

A. Ground 1: Claims 1-15 are unpatentable under 35 U.S.C. § 103(a) as obvious in view of Abad and Piccard.

Petitioner evaluates the scope and content of the prior art, any differences between the art and the claim, and the knowledge of person of ordinary skill in the art in accordance with *Graham v. John Deere Co.*, 383 U.S. 1 (1966) and *KSR Int'l Co. v. Teleflex, Inc.*, 550 U.S. 398 (2007). Petitioner is unaware of any secondary considerations relevant to the '932 patent and a more than adequate written rationale is provided to support the combination of Halperin and Inoue under *KSR*. 550 U.S. at 418.

A PHOSITA would have been motivated to combine Abad with Piccard because both references address the same problem, identifying malware in computer systems, and do so in a compatible manner. EX1006, p.1,5; EX1003, ¶¶95-96,105-106,117; EX1007, ¶¶[0019]-[0020].

Abad is directed toward detecting malicious or unwanted behavior, i.e., “pestware,” and does so through the correlation of logs that record multiple sources of computer activity information beyond system calls and network activity. EX1003, ¶¶118-121; EX1006, p.6. Abad recognizes the efficiency and accuracy in identifying malware gained through correlating multiple sources of activity information and teaches correlating information on a network level. *Id.* While

Abad's system focuses on the "Detection" stage, Abad anticipates the need for post-detection responses, such as coordinated research or notification to other parties on the network. *Id.* at ¶122.

Piccard, in the same field of endeavor, discloses methods for detecting malware, particularly identifying the source of malware, using identification and reporting modules, including a "malware detection module." EX1003, ¶¶123-124. Piccard teaches identifying the origin of malware (e.g., a URL) and sharing that information with a research entity in order to provide better detection capabilities to nodes on the network. EX1003, ¶124. Thus, Piccard complements the disclosure in Abad by disclosing methods for identifying sources of malware to enable blacklisting and updating malware definitions "to account for evolving malware." EX1007, ¶[0003]; EX1003, ¶126.

A PHOSITA would have been motivated to combine the teachings of Piccard with Abad because Abad identifies a need for post-detection reaction to intrusions and Piccard's "Web site identification module" and "reporting module" provide solutions for responding to suspected malware in order to prevent its recurrence. EX1003, ¶122. For example, Abad says "[p]roblems should be fixed, intruders stopped, and data restored." EX1006, p.2. Also, Abad teaches the value of correlating multiple types of activity information (see EX1006, pp.2-3), and a PHOSITA would have viewed Piccard's disclosures of using web history logs to

determine the source of suspected malware as a further source of activity information. EX1003, ¶128. Abad is also clear that relevant information about malicious activity is available across the network, and that such information should be examined together and used to improve the security of the entire network, information that Piccard's systems provide. EX1003, ¶¶124-128.

A PHOSITA would have recognized that Abad's teachings of detecting suspected malware through behavior monitoring align with Piccard's disclosures of its "malware detection module". EX1003, ¶125. Because Piccard discloses the "malware detection module" as a discrete component with multiple possible implementations but a defined output (i.e., the suspected file), a PHOSITA would have had a high expectation of success implementing Abad's techniques as part of Piccard's malware detection module and vice versa. *Id*

1. Claim 1

a. A method for identifying an origin of activity on a computer that is indicative of pestware comprising:

Abad and Piccard both teach this preamble. Abad is directed toward detecting malicious or unwanted behavior through the correlation of multiple logs. EX1006, pp.1-2; EX1003, ¶¶132-134. Piccard teaches a process for protecting a computing device and including operations or methods to determine the source of malware acting on the system (corresponding to "identifying an origin of activity

on a computer”). EX1006, ¶¶[0005],[0019]-[0023]; EX1003, ¶¶134-135. Thus, Abad discloses this claim preamble. *Id.* at ¶136.

b. monitoring, using a kernel-mode driver, API call activity on the computer;

Abad teaches using a system monitor called APISpy32 (corresponding to “kernel-mode driver”) to monitor the system “from the kernel level by recording the system calls executed by the system”, which corresponds to “monitoring ... API call activity on the computer”. EX1006, p.6; EX1003, ¶139. These system calls are data mined for indicators of malware (corresponding to “monitoring...API call activity on the computer”) and to enable the monitor to evaluate when new processes are launched. EX1006, pp.5-6; EX1003, ¶¶67-69,139. Specifically, Abad states “[t]he logged system calls and network traffic on the client machine were then mined to determine if an intrusion had taken place.” EX1006, pp.5-6.

Thus, Abad renders this limitation obvious. EX1003, ¶140.

c. storing information related to the API call activity in a log;

Abad teaches storing (e.g., “logging” or “recording”) monitored system calls, such as Windows API calls: “Our architecture consists of logging utilities that monitor system activity from different vantage points. For example, APISpy32 [10] monitors the system from the kernel level by recording the system calls

executed by the system.” EX1006, p.6; EX1003, ¶143. A PHOSITA would have understood that Windows system calls, such as those being recorded by a monitor like APISpy32, are “API calls” as recited in this limitation. EX1003, ¶143. Thus, Abad discloses this limitation. *Id.* at ¶144.

d. analyzing, heuristically, the API call activity to determine whether one or more weighted factors associated with the API call activity exceeds a threshold;

Abad teaches that the core data mining tool (called RIPPER) used in the identification of malware in a bottom-up method of detection is trained based on collected system calls including normal and abnormal system calls (corresponding to “analyzing, heuristically, the API call activity”). EX1006, pp.5,8; EX1003, ¶¶147-148. This training results in the creation or identification of rules that can be learned and used by the system to identify malware. *Id.* Each of these rules is associated with a confidence level which indicates the ratio of matched to total samples (corresponding to “analyzing, heuristically, the API call activity”). *Id.* Based on these rules and confidence levels, the system predicts for new samples whether a series of events are anomalous indicating malware. EX1006, p.6; EX1003, ¶¶149-150. In addition, Abad incorporates likelihoods, penalties, sliding windows, and thresholds into this decision making (corresponding to “to determine whether one or more weighted factors associated with the API call activity exceeds

a threshold”) any of which a PHOSITA would understand to be heuristics.

EX1006, p.7; EX1003, ¶¶151-154.

Accordingly, Abad teaches these limitations. EX1003, ¶155.

e. identifying, based upon the API call activity, a suspected pestware object on the computer;

Abad teaches a logging architecture that monitors a computer system from a number of vantage points to identify abnormal behavior (corresponding to “identifying, based upon the API call activity, a suspected pestware object on the computer”). EX1006, p.6; EX1003, ¶¶158-159. As noted regarding the limitation of claim 1[b], this logging architecture includes logs of system calls which a PHOSITA would have understood to identify processes (programs / executables) and their process ID. *Id.* Further, a PHOSITA would have understood that process IDs (PIDs) can be traced to the executable file and file name (e.g., file path) by simple OS utilities. EX1003, ¶¶71-75, 159-160 (citing EX1012)(citing EX1011). Accordingly, a PHOSITA would have found processes and executable objects interchangeable for identification purposes (corresponding to “identifying, based upon the API call activity, a suspected pestware object on the computer”). *Id.*

Accordingly, a PHOSITA would have found this limitation to be obvious based on Abad. EX1003, ¶161.

f. 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

Abad discloses correlating network traffic logs (corresponding to “a recorded history of externally networked sources that the computer received files from”) with system calls that are abnormal. EX1006, pp.2,5; EX1003, ¶164. In this manner, the system of Abad can identify the process, network traffic, or email (and, therefore, the executable file) that the malicious system call originated from. EX1006, pp.2,5; EX1003, ¶¶71-75,165-167. Accordingly, Abad can link an email or network event to a system call or a process via correlation, which corresponds to “identifying, in response to the identifying the suspected pestware object, a reference of an externally networked source of the suspected pestware object”.

Further, Piccard also teaches storing and accessing file download history logs from a web browser in order to identify a web site that was the source of the malicious file. EX1007, pp.2,5; EX1003, ¶¶168-169. A PHOSITA would have been motivated to incorporate the download history log of Piccard via predictable methods into the log aggregator of Abad at least because Abad recognized that file downloads were a source of malware. EX1006, p.5; EX1007, ¶¶[0015],[0017],[0019]; EX1003, ¶¶63-66,170-171 (citing EX1010). A POSITA would have found Piccard's logs to be compatible with Abad's correlation and data mining techniques. *Id.*

Therefore, a PHOSITA would have found these limitations to be obvious based on Abad and Piccard.EX1003, ¶172.

g. reporting the identity of the externally networked source to an externally networked pestware research entity,

Abad teaches that log aggregation and correlation typically takes place at a central point or centralized correlation engine. EX1006, p.3; EX1003, ¶¶175-176. Further, Piccard teaches a reporting module that reports information regarding the downloaded file, its source, and other relevant information (e.g., file name) to a remotely-located computer in the computer network of the protected / monitored computer (corresponding to “reporting the identity of the externally networked source to an externally networked pestware research entity”). EX1007, ¶[0015]; EX1003, ¶¶177-178. The remote computer of Piccard then analyzes the relevant information. EX1007, ¶[0023]; EX1003, ¶179.

Therefore, a PHOSITA would have found these limitations to be obvious based on Abad and Piccard.EX1003, ¶180.

h. 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.

Abad teaches the need to correlate information on a network level, a concept taught by Piccard’s identification and reporting modules. Piccard teaches identifying the origin of pestware, disclosing a “Web site identification module”

that is invoked after a determination of malware by the “malware detection module”, which accesses the history log to determine the external source of the object. EX1003, ¶183; EX1007, ¶[0015]. More particularly, Piccard discloses that the recorded “Web address of the file” can be a web URL or an IP address. EX1003, ¶¶183-184; EX1007, ¶[0013],[0021]. A PHOSITA would have understood that a URL can be converted to an IP address via any domain name system (DNS) server which was readily available at the time. EX1003, ¶185.

Therefore, a PHOSITA would have found these limitations to be obvious based on Abad and Piccard. EX1003, ¶¶186-187. Therefore, a PHOSITA would have found claim 1 to be obvious based on the Abad-Piccard combination. Accordingly, claim 1 should be found invalid under 35 U.S.C. § 103 based on Abad and Piccard.

2. Claim 2

The method of claim 1, wherein the identifying the suspected pestware object includes accessing an activity log that includes information that relates the activity to the suspected pestware object.

Abad discloses monitoring activity logs of the computer including system call logs (e.g., by APISpy32). EX1006, pp.5,6; EX1003, ¶¶189-190. A PHOSITA would have understood that system call logs will include information that relates to the activity. EX1003, ¶190. A PHOSITA would have known it to be possible, and would have found it obvious, to identify the file (the “suspected pestware object”)

from which the process was launched. *Id.* The system call logs include traceable logs that allow a next system call to be predicted. *Id.* A PHOSITA would have understood a traced series of events or calls to relate to the activity of a particular object. EX1003, ¶¶190-191.

Therefore, a PHOSITA would have found the limitation recited claim 2 to be obvious based on Abad. EX1003, ¶192. As shown, the Abad-Piccard combination discloses all elements recited in claim 1 from which claim 2 depends. Accordingly, claim 2 should be found invalid under 35 U.S.C. § 103 based on Abad and Piccard.

3. Claim 3

The method of claim 1, wherein the identifying a reference includes accessing at least a portion of a recorded history of externally networked sources.

Piccard discloses that when malware is identified on a computer, the website identification module of Piccard uses the download history of the web browser to identify the network source of the file (corresponding to “at least a portion of a recorded history of externally networked sources”). EX1007, ¶¶[0021]-[0022]; EX1003, ¶194. Piccard discloses that the web browser’s history log stores information identifying a listing of times, URLs, and objects that were downloaded. EX1003, ¶194.

Therefore, a PHOSITA would have found the limitation recited claim 3 to be obvious based on Piccard. EX1003, ¶¶195-196. As shown, the Abad-Piccard combination discloses all elements recited in claim 1 from which claim 3 depends. Accordingly, claim 3 should be found invalid under 35 U.S.C. § 103 based on Abad and Piccard.

4. Claim 4

The method of claim 3, 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.

As described regarding claim limitation 1[c], Abad discloses monitoring network traffic and collecting a network log that is used to identify malware (corresponding to “an activity log”, “an event log”, or “monitoring software logs”). EX1006, p.2; EX1003, ¶¶143,198.

Piccard teaches a accessing a web browser’s history log that includes file download history from external websites and other salient information, which corresponds to “the recorded history resides in at least one log selected from the group consisting of ...a browser history, browser cache.” EX1007, ¶¶[0021]-[0022]; EX1003, ¶¶200-205. A PHOSITA would have recognized the web browser’s history log of Piccard stores information identifying a listing of times, URLs, and objects that were downloaded as a browser’s cache. EX1003, ¶203.

Therefore, a PHOSITA would have found the limitation recited claim 4 to be obvious based on Abad or Abad and Piccard. EX1003, ¶¶205-207. As shown, the Abad-Piccard combination discloses all elements recited in claims 1 and 3 from which claim 4 depends. Accordingly, claim 4 should be found invalid under 35 U.S.C. § 103 based on Abad and Piccard.

5. Claim 5

a. A system for identifying a source of activity on a computer that is indicative of pestware including:

Abad and Piccard both teach this preamble. EX1003, ¶210. Abad is directed toward detecting malicious or unwanted behavior on a computer through the correlation of multiple logs. EX1006, pp.1,5; EX1003, ¶211-212. Piccard teaches a process for protecting a computing device and including operations or methods to determine the source of malware acting on the system (corresponding to “identifying a source of activity on a computer that is indicative of pestware”). EX1007, ¶¶[0005],[0012],[0019]-[0023]; EX1003, ¶213-215.

b. 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;

Abad teaches using a system call monitor (corresponding to “configured to monitor API call activity monitor”) called APISpy32 (corresponding to a “kernel-level monitor”) to monitor the system “from the kernel level by recording the

system calls executed by the system”, which corresponds to “configured to monitor API call activity on the computer and to store information related to the API call activity in a log”. EX1006, p.6; EX1003, ¶219. These system call logs are data mined for indicators of malware and to enable the monitor to evaluate when new processes are launched. EX1006, pp.5-6; EX1003, ¶¶67-69,219. Specifically, Abad states “[t]he logged system calls and network traffic on the client machine were then mined to determine if an intrusion had taken place.” *Id.* Likewise, Abad explains “[w]e used APISpy32 [10], with some modification, to intercept system calls,” which corresponds to “a kernel-level monitor configured to monitor API call activity.” EX1006, p.5; EX1003, ¶219.

Therefore, a PHOSITA would have found these limitations to be obvious based on Abad. EX1003, ¶220.

c. 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;

This limitation is equivalent to limitation 1[d] differing only in reciting “a heuristics module configured to analyze.” As discussed regarding claim limitation 1[d], Abad teaches that the core data mining tool called RIPPER (corresponding to a “heuristics module”) used in the identification of malware in a bottom-up method of detection is trained based on collected system calls including normal and abnormal system calls (corresponding to “configured to analyze the API call

activity”). EX1006, pp.5,8; EX1003, ¶¶223-225. This training results in the creation or identification of rules that can be learned and used by the system to identify malware. *Id.* Each of these rules is associated with a confidence level which indicates the ratio of matched to total samples. *Id.* Based on these rules and confidence levels, the system predicts for new samples whether a series of events are anomalous indicating malware. EX1006, p.6; EX1003, ¶¶226-227. In addition, Abad incorporates likelihoods, penalties, sliding windows, and thresholds into this decision making (corresponding to “analyze the API call activity to determine whether one or more weighted factors associated with the API call activity exceeds a threshold”). EX1006, p.7; EX1003, ¶¶226-229.

Therefore, a PHOSITA would have found these limitations to be obvious based on Abad. EX1003, ¶230.

d. a research portion configured to identify, in response to a prompt from the heuristics module, a suspected pestware object on the computer; and

This claim limitation is similar to limitation 1[e]. As described regarding claim limitation 1[e], Abad teaches a logging architecture including RIPPER (corresponding to “a research portion”) that monitors a computer system from a number of vantage points to identify abnormal behavior (corresponding to “configured to identify... a suspected pestware object”). EX1006, p.5-6; EX1003, ¶233. A PHOSITA would have understood that process IDs (PIDs) can be traced

to the executable file and file name (e.g., file path) by simple OS utilities. EX1003, ¶¶71-74,234 (citing EX1012)(citing EX1011)(citing EX1009)(citing EX1014). A PHOSITA would have found processes and executable objects interchangeable for identification purposes (corresponding to “identify a suspected pestware object on the computer”). *Id.* Similarly, the purpose of Piccard’s “Web site identification module” is to associate the suspicious file with its URL source. EX1003, ¶¶235-236. Further, Piccard teaches that its “Web site identification module” starts its search of the history log after determination by the “malware detection module” that a file includes potential malware (corresponding to “a research portion configured to identify, in response to a prompt from the heuristics module”). EX1007, ¶[0021]; EX1003, ¶¶235-238. A POSITA would have found Piccard's logs to be compatible with Abad's correlation and data mining techniques. *Id.*

Therefore, a PHOSITA would have found these limitations to be obvious based on Abad and Piccard. EX1003, ¶239.

- e. 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,**

This limitation is similar to a combination of limitations 1[e], 1[f] and 1[g]. Abad teaches that log aggregation and correlation typically takes place at a central point or centralized correlation engine. EX1006, p.3; EX1003, ¶242. Further,

Piccard teaches a reporting module that reports information (corresponding to “a reporting portion configured to generate a report”) regarding the downloaded file, its source, and other relevant information (e.g., file name) to a remotely-located computer in the computer network of the protected / monitored computer (corresponding 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”). EX1007, ¶[0015]; EX1003, ¶¶243-244. The remote computer of Piccard then analyzes the relevant information. EX1007, ¶[0023]; EX1003, ¶243.

Therefore, a PHOSITA would have found these limitations to be obvious based on Abad and Piccard. EX1003, ¶245.

f. wherein 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.

As described regarding limitation 1[d], Abad teaches that the RIPPER core data mining tool used in the identification of malware in a bottom-up method of detection is trained based on collected system calls including normal and abnormal system calls. EX1006, pp.5,8; EX1003, ¶219,248. Abad teaches correlating logs to identify links between computer activities, such as network activity and system call activity. EX1006, p.5-6. In the combination of Abad-Piccard, this network activity would include files downloaded from the Internet. EX1006, p.5-6;

EX1003, ¶248. Thereafter, since the stored activity includes the API call and the process identity associated with the call, a PHOSITA would have found it obvious that the logs of Abad and Piccard would identify the file corresponding to the API call (e.g., by storing the information together in the activity in the log, or by looking up the stored file name based on the process ID stored in the activity log). EX1003, ¶¶71-75,248 (citing EX1011). Therefore, Abad in view of Piccard renders limitation 5[f] obvious. *Id.* at ¶249.

Therefore, a PHOSITA would have found claim 5 to be obvious based on the Abad-Piccard combination. Accordingly, claim 5 should be found invalid under 35 U.S.C. § 103 based on Abad and Piccard.

6. Claim 6

The system of claim 5, wherein the information comprises an identity of at least one process that made at least one API call in the log.

A PHOSITA would have understood that system call logs of Abad identify the process that made the system call (e.g., through a “handle” or “process ID”). EX1006, pp.5,8; EX1003, ¶¶71-75,252. Because the API calls being logged by the Abad-Piccard system represent system calls, a PHOSITA would have understood that these logs contain at least the process ID identifying the process that made the system call. *Id.*

Therefore, a PHOSITA would have found the limitation in claim 6 to be obvious based on Abad in view of Piccard. EX1003, ¶253. As shown, the Abad-

Piccard combination discloses all elements recited in claim 5 from which claim 6 depends. Accordingly, claim 6 should be found invalid under 35 U.S.C. § 103 based on Abad and Piccard.

7. Claim 7

The system of claim 5, 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.

As described regarding the limitations of claim 1[b], Abad teaches a system call monitor called APISpy32 (corresponding to “information about the API call activity from the kernel-level monitor”) that intercepts system calls and logs them in an aggregated logging architecture to be data mined for correlations by RIPPER (corresponding to “the heuristics module”). EX1006, pp.5-6; EX1003, ¶¶255-259. Further, as also noted above, Abad teaches that the software module called RIPPER performs data mining on the system call logs and other logs received from the monitors to identify abnormal activity and trace it to a malicious process (corresponding to “to determine whether the API call activity is indicative of pestware”). *Id.*

Therefore, a PHOSITA would have found the limitation recited claim 7 to be obvious based on Abad and Piccard. EX1003, ¶260. As shown, the Abad-Piccard combination discloses all elements recited in claim 5 from which claim 7 depends.

Accordingly, claim 7 should be found invalid under 35 U.S.C. § 103 based on Abad and Piccard.

8. Claim 8

The system of claim 5, wherein the kernel-level monitor is configured to intercept at least one API call.

Abad teaches monitoring multiple system calls, including Windows API calls, at the kernel level, and is explicit that such monitoring is done by intercepting system calls. EX1003, ¶262. “We used APISpy32 [10], with some modification, to intercept system calls. The logged system calls and network traffic on the client machine were then mined to determine if an intrusion had taken place.” EX1006, p.5. A PHOSITA would have understood that Windows system calls, such as recorded by a monitor like APISpy32, relate to the claimed “API call” recited in this claim. EX1003, ¶¶263-264.

Therefore, a PHOSITA would have found the limitation recited claim 8 to be obvious based on Abad and Piccard. *Id.* at ¶265. As shown, the Abad-Piccard combination discloses all elements recited in claim 5 from which claim 8 depends. Accordingly, claim 8 should be found invalid under 35 U.S.C. § 103 based on Abad and Piccard.

9. Claim 9

The system of claim 5, 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.

Claim 9 is equivalent to limitation 1[h]. As shown for 1[h], Abad teaches the need to correlate information on a network level, a concept taught by Piccard's identification and reporting modules. Piccard discloses that the recorded "Web address of the file" can be a web URL or an IP address. EX1003, ¶¶267-268; EX1007, ¶[0013],[0021]. Further, a PHOSITA would have understood that a URL can be converted to an IP address via any domain name system (DNS) server which was readily available at the time. EX1003, ¶269.

Accordingly, the combination of Abad and Piccard renders claim 9 limitations obvious. EX1003, ¶270. As shown, the Abad-Piccard combination discloses all elements recited in claim 5 from which claim 9 depends. Accordingly, claim 9 should be found invalid under 35 U.S.C. § 103 based on Abad and Piccard.

10. Claim 10

The system of claim 5, wherein the research portion is configured to access at least a portion of a recorded history of externally networked sources.

Claim 10 is equivalent to claim 3. Abad describes collecting network logs and network activity / traffic to assist in tracing intrusions. EX1006, pp.3,5; EX1003, ¶¶272-274. Further, Piccard discloses that when malware is identified on a computer, the website identification module of Piccard uses the download history of the web browser to identify the network source of the file (corresponding to “the research portion is configured to access at least a portion of a recorded history of externally networked sources”). EX1007, ¶¶[0021]-[0022]; EX1003, ¶¶275-276. Further, Piccard teaches a reporting information to a remotely-located computer in the computer network of the protected / monitored computer (corresponding to “access[ing] at least a portion of a recorded history of externally networked sources”). EX1007, ¶[0015]; EX1003, ¶¶275-276.

Therefore, a PHOSITA would have found the limitation recited claim 10 to be obvious based on Piccard. EX1003, ¶277. As shown, the Abad-Piccard combination discloses all elements recited in claim 5 from which claim 10 depends. Accordingly, claim 10 should be found invalid under 35 U.S.C. § 103 based on Abad and Piccard.

11. Claim 11

The system of claim 10, 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.

The claim 11 limitations are equivalent to limitations in claim 4. As described regarding claim 4, Abad discloses monitoring network traffic and collecting a network log that is used to identify malware (corresponding to “an activity log”, “an event log”, or “monitoring software logs”). EX1006, p.2; EX1003, ¶¶281-282.

Piccard teaches a accessing a web browser’s history log that includes file download history from external websites and other salient information, which a PHOSITA would recognize corresponds to “the recorded history resides in at least one log selected from the group consisting of ...a browser history, browser cache.” EX1007, ¶¶[0021]-[0022]; EX1003, ¶¶279-280.

Therefore, a PHOSITA would have found the limitation recited claim 4 to be obvious based on Abad or Abad and Piccard. EX1003, ¶283. As shown, the Abad-Piccard combination discloses all elements recited in claims 5 and 10 from which claim 11 depends. Accordingly, claim 11 should be found invalid under 35 U.S.C. § 103 based on Abad and Piccard.

12. Claim 12

- a. 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:**

The preamble of claim 12 is similar to the preamble of claim 1 except that it recites a “non-transitory computer-readable medium including processor-executable instructions for” instead of “method.” As discussed regarding claim limitations 1[a] and 5[a], Abad and Piccard both disclose computer systems and computer-implemented methods of malware detection. A PHOSITA would have known that methods executing on a computer are implemented as executable instructions that load into a processor from a non-transitory tangible computer readable storage medium, such as a hard drive. EX1003, ¶¶287-291. Accordingly, Abad and Piccard teach the preamble. EX1003, ¶292.

The limitations of claim 12 are otherwise identical to the limitations in claim 1, with a small exception in the final limitation 12[h]. EX1003, ¶293. Therefore, in the analysis of claim 12 reference is made to the corresponding limitation discussions in claim 1.

- b. monitoring, using a kernel-mode driver, API call activity on the computer;**

As shown re 1[b], a PHOSITA would have found this limitation to be obvious based on Abad. EX1003, ¶¶140,293.

c. storing information related to the API call activity in a log;

As shown re 1[c], a PHOSITA would have found this limitation to be obvious based on Abad. EX1003, ¶144,293.

d. analyzing, heuristically, the API call activity to determine whether one or more weighted factors associated with the API call activity exceeds a threshold;

As shown re 1[d], a PHOSITA would have found this limitation to be obvious based on Abad. EX1003, ¶155,293.

e. identifying, based upon the API call activity, a suspected pestware object on the computer;

As shown re 1[e], a PHOSITA would have found this limitation to be obvious based on Abad. EX1003, ¶161,293.

f. 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

As shown re 1[f], the combination of Abad and Piccard renders this limitation obvious. EX1003, ¶172,293.

g. reporting the identity of the externally networked source to an externally networked pestware research entity, wherein

As shown re 1[g], the combination of Abad and Piccard renders this limitation obvious. EX1003, ¶180,293.

h. 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.

As shown re 1[h], Abad teaches this limitation the addition of the words “selected by an identifier.” EX1003, ¶¶183-184,293. The identifiers listed in 12[h] include a URL and an IP address. As shown re 1[h], Piccard discloses that the recorded “Web address of the file” can be a web URL or an IP address. EX1003, ¶183-184; EX1007, ¶[0013],[0021]. A PHOSITA would have understood that a URL can be converted to an IP address via any domain name system (DNS) server which was readily available at the time. EX1003, ¶185. Thus, the combination of Abad and Piccard renders this limitation obvious. EX1003, ¶186.

Therefore, a PHOSITA would have found claim 12 to be obvious based on the Abad-Piccard combination. Accordingly, claim 12 should be found invalid under 35 U.S.C. § 103 based on Abad and Piccard.

13. Claim 13

The non-transitory computer-readable medium of claim 12, wherein the instructions for identifying the suspected pestware object include instructions for accessing an activity log that includes information that relates the activity to the suspected pestware object.

Other than reciting the non-transitory computer-readable medium, claim 13 is essentially identical to claim 2. As shown regarding claim 2, a PHOSITA would have found the limitation recited claim 13 to be obvious based on Abad. EX1003,

¶296. As shown, the Abad-Piccard combination discloses all elements recited in claim 12 from which claim 13 depends. Accordingly, claim 13 should be found invalid under 35 U.S.C. § 103 based on Abad and Piccard.

14.Claim 14

The non-transitory computer-readable medium of claim 12, wherein the instructions for identifying a reference include instructions for accessing at least a portion of a recorded history of externally networked sources.

Other than reciting the non-transitory computer-readable medium, claim 14 is essentially identical to claim 3. As shown regarding claim 3, a PHOSITA would have found the limitation recited claim 14 to be obvious based on Piccard.

EX1003, ¶298. As shown, the Abad-Piccard combination discloses all elements recited in claim 12 from which claim 14 depends. Accordingly, claim 14 should be found invalid under 35 U.S.C. § 103 based on Abad and Piccard.

15. Claim 15

The non-transitory computer-readable medium of claim 14, 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.

Other than reciting the non-transitory computer-readable medium, claim 13 is essentially identical to claim 4. As shown regarding claim 4, a PHOSITA would have found the limitation recited claim 15 to be obvious based on Abad or Abad

and Piccard. EX1003, ¶300. As shown, the Abad-Piccard combination discloses all elements recited in claims 12 and 14 from which claim 15 depends.

Accordingly, claim 15 should be found invalid under 35 U.S.C. § 103 based on Abad and Piccard.

B. Ground 2: Claims 1-15 are unpatentable under 35 U.S.C. § 103 as obvious by Kilpatrick in view of Piccard.

Ground 2 is evaluated under the same standards as Ground 1 summarized above.

A PHOSITA would have been motivated to combine Kilpatrick with Piccard because both references address the same problem, identifying malware in computer systems, and do so in a compatible manner. EX1003, ¶¶302-309; EX1008, 4:17-55; EX1007, ¶¶[0019]-[0020].

Kilpatrick is directed toward detecting anomalous behavior through monitoring system calls and comparing them with a program-specific distance matrix. EX1003, ¶¶112-118,302. Kilpatrick discloses the use of wrapper specifications (i.e., criteria to specify when a wrapper should be loaded) that anticipate particular directories being useful targets for monitoring for malware “because the interception occurs inside the kernel [so] the wrappers cannot be bypassed by malicious code.” EX1008, 4:56-62; EX1003, ¶¶112-118,303.

Kilpatrick also teaches that various actions may be taken to mitigate the impact of malicious code once it is detected. *Id.* at ¶¶112-118,304; EX1008, 11:22-28.

Piccard, in the same field of endeavor, discloses methods for detecting malware, particularly teaches steps to take after identification of malware downloaded from an external source. EX1003, ¶¶108-111,307; EX1007, ¶[0003]. Piccard teaches a “malware detection module” as the first operation in its method “to analyze a file to determine that the file includes potential malware (block 200).” EX1007, ¶[0019]. Thus, Piccard complements the disclosure in Kilpatrick by disclosing methods for identifying sources of malware to enable blacklisting and updating malware definitions “to account for evolving malware”. EX1003, ¶¶308-309; EX1007, ¶[0003],[0014].

A PHOSITA would have been motivated to combine the teachings of Piccard with Kilpatrick because Kilpatrick identifies that various actions may be taken to mitigate the impact of malicious code once it is detected and Piccard’s “Web site identification module” provides solutions for responding to suspected malware in order to prevent its recurrence. EX1003, ¶¶305-309.

A PHOSITA would have recognized that Kilpatrick’s teachings of detecting suspected malware through system call monitoring align with Piccard’s disclosures of its “malware detection module”. *Id.* Because Piccard discloses the “malware detection module” as a discrete component with multiple possible implementations

but a defined output (i.e., the suspected file), a PHOSITA would have had a high expectation of success implementing Kilpatrick's techniques as part of Piccard's malware detection module and vice versa. *Id.*

1. Claim 1

a. A method for identifying an origin of activity on a computer that is indicative of pestware comprising:

Kilpatrick and Piccard both teach this preamble. Kilpatrick is directed toward a method that monitors applications for anomalous behavior in order to detect intrusions and processes responsible. EX1008, 1:9-27,4:15-25; EX1003, ¶¶313-314. Piccard teaches a process for protecting a computing device and including operations or methods to determine the source of malware acting on the system (corresponding to "identifying an origin of activity on a computer"). EX1007, ¶¶[0019]-[0023]; EX1003, ¶315.

b. monitoring, using a kernel-mode driver, API call activity on the computer;

Kilpatrick teaches a "kernel-loadable module [that] intercepts all system calls as they are made by a program," which corresponds to "monitoring, using a kernel-mode driver, API call on the computer." EX1003, ¶320; EX1008, 4:33-55. Kilpatrick notes that these intercepts occur in the kernel or at the kernel level.

EX1003, ¶321; EX1008, 4:59-62, 12:3-6. A PHOSITA would have understood that these system calls intercepted at the kernel level would include API calls which are calls that allow user-space applications to call into kernel space (corresponding to “the monitoring includes monitoring API calls”). EX1003, ¶¶322-323 (citing EX1013, p.1). Finally, Kilpatrick teaches that these system calls are stored and viewable in a sliding event window showing recent history of system calls. EX1003, ¶323; EX1008, 8:33-38.

Therefore, a PHOSITA would have found these limitations to be obvious based on Kilpatrick. EX1003, ¶324.

c. storing information related to the API call activity in a log;

Kilpatrick teaches that the intercepted system calls are stored in a sliding window log of recent system calls for further analysis. EX1003, ¶327; EX1008, 8:33-45. Therefore, a PHOSITA would have found these limitations to be obvious based on Kilpatrick. *Id.* at ¶328.

d. analyzing, heuristically, the API call activity to determine whether one or more weighted factors associated with the API call activity exceeds a threshold;

Kilpatrick teaches that the intercepted system calls are stored in a sliding window log of recent system calls for further analysis. EX1003, ¶331; EX1008, 8:33-45. Kilpatrick analyzes each system call pair that is inserted into the event

window based on a distance matrix to determine if the sequence is anomalous (corresponding to “analyzing, heuristically, computer activity to ...arrive at a determination that the activity is indicative of pestware”). EX1003, ¶¶332-333; EX1008, 8:25-40. If the sequence is new, the detect process will measure the magnitude of the difference between several known sequences in the distance matrix and the intercepted system call and compare to a predefined threshold. EX1003, ¶¶332-334; EX1008, 9:8-23. A PHOSITA would have understood comparing a number of distance values against a predefined threshold by using Kilpatrick’s ‘minimum value’ involves weighting the other values. EX1008, 11:19-28; EX1003, ¶335.

Therefore, a PHOSITA would have found these limitations to be obvious based on Kilpatrick. EX1003, ¶336.

e. identifying, based upon the API call activity, a suspected pestware object on the computer;

Kilpatrick teaches intercepting all system calls by a program and tracking running processes via the system calls. EX1003, ¶¶339-340; EX1008, 4:35-55. A PHOSITA would have known it to be possible, and would find it obvious and routine, to identify the executable file from which the process was launched (corresponding to “identifying, based upon the API call activity, a suspected

pestware object on the computer”). EX1003, ¶¶71-75,340. This executable file would then represent the source of the activity, and a POSITA would have understood process ID and file locations / paths to be common convertible identifiers for executable programs. EX1003, ¶¶71-75,341.

Therefore, a PHOSITA would have found this limitation to be obvious based on Kilpatrick. EX1003, ¶ 342.

f. 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

Piccard teaches a malware detection module and a website identification module. EX1003, ¶¶345-346; EX1007, ¶¶[0014]-[0015]. The malware detection module of Piccard analyzes files that have been downloaded and, in the combined Kilpatrick-Piccard system, analyzes files identified as the sources of anomalous system call sequences as described regarding claim limitations 1[c] and 1[d]. EX1003, ¶¶345-346; EX1007, ¶¶[0014]-[0015].

Further, Piccard also teaches storing and accessing file download history logs from a web browser in order to identify a web site (corresponding to “a reference to an identity of an externally networked source”) that was the source of the malicious file. EX1007, pp.2,5; EX1003, ¶¶345-348. A PHOSITA would have been motivated to incorporate the download history log of Piccard via predictable

methods into the malicious program detector of Kilpatrick. EX1008, 4:17-45; EX1007, ¶¶[0015],[0017],[0019]; EX1003, ¶¶63-66,348 (citing EX1010).

Therefore, a PHOSITA would have found this limitation to be obvious based on Kilpatrick and Piccard. EX1003, ¶349.

g. reporting the identity of the externally networked source to an externally networked pestware research entity, wherein

Piccard teaches a reporting module that reports information regarding the downloaded file, its source, and other relevant information (e.g., file name) to a remotely-located computer in the computer network of the protected / monitored computer (corresponding to “reporting the identity of the particular externally networked source to an externally networked pestware research entity”). EX1007, ¶[0015]; EX1003, ¶¶352-353. The remote computer of Piccard then analyzes the relevant information “to determine whether the file does, in fact, include malware and whether the Web site is, in fact, a malware distribution site.” EX1007, ¶[0023]; EX1003, ¶353. A PHOSITA would understand that this analysis corresponds to “so as to enable the externally networked pestware research entity to research whether the particular externally networked source is a source of pestware”. EX1003, ¶¶354-355.

Therefore, a PHOSITA would have found these limitations to be obvious based on Piccard. EX1003, ¶355.

- h. 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.**

Piccard teaches identifying the origin of pestware, disclosing a “Web site identification module” that is invoked after a determination of malware by the “malware detection module”, which accesses the history log to determine the external source of the object. EX1003, ¶358; EX1007, ¶[0015]. More particularly, Piccard discloses that the recorded “Web address of the file” can be a web URL or an IP address. EX1003, ¶359; EX1007, ¶[0013],[0021]. A PHOSITA would have understood that a URL can be converted to an IP address via any domain name system (DNS) server which was readily available at the time. EX1003, ¶360. Therefore, a PHOSITA would have found these limitations to be obvious based on Piccard. EX1003, ¶¶361-362.

Therefore, a PHOSITA would have found claim 1 to be obvious based on the Kilpatrick-Piccard combination. Accordingly, claim 1 should be found invalid under 35 U.S.C. § 103 based on Kilpatrick and Piccard.

2. Claim 2

The method of claim 1, 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 described regarding claim limitation 1[e], Piccard discloses identifying the web site that was the source of a file downloaded via a web browser using the web browser download history (corresponding to “the identifying the suspected pestware object includes accessing an activity log that includes information”). EX1007, ¶[0015]; EX1003, ¶¶339-342. Further, Piccard discloses that the recorded web address of the identified source website can be a web URL or an IP address. EX1007, ¶[0021]; EX1003, ¶359. A PHOSITA would have understood that a URL can be converted to an IP address via any domain name system (DNS) server which was readily available at the time. EX1003, ¶360.

Therefore, a PHOSITA would have found the limitation recited claim 2 to be obvious based on Piccard. EX1003, ¶366. As shown, the Kilpatrick-Piccard combination discloses all elements recited in claim 1 from which claim 2 depends. Accordingly, claim 2 should be found invalid under 35 U.S.C. § 103 based on Kilpatrick and Piccard.

3. Claim 3

The method of claim 1, wherein the identifying a reference includes accessing at least a portion of a recorded history of externally networked sources.

As explained above, Kilpatrick discloses monitoring system calls as they are generated by processes interacting with the operating system. EX1003, ¶346; EX1008, 4:37-55. In addition, a PHOSITA would have understood that system call logs, such as those taught by Kilpatrick, identify the process that made the system call. EX1003, ¶365; EX1008, 4:37-55. A PHOSITA would have known it to be possible, and would find it obvious and routine, to identify the file from which the process was launched. EX1003, ¶¶71, 74 (citing EX1011 and EX1012). Thus, a PHOSITA would have understood the system calls intercepted for a given program to be related to the activity of the object (e.g., file) identified.

Further, Piccard discloses that when malware is identified on a computer, the website identification module of Piccard uses the download history of the web browser to identify the network source of the file (corresponding to “at least a portion of a recorded history of externally networked sources”). EX1007, ¶¶[0021]-[0022]; EX1003, ¶¶368-369. A PHOSITA would have understood that the web browser’s history log of Piccard stores information that would be in a “browser cache” (e.g., a listing of times, URLs, and objects that were downloaded). EX1003, ¶¶369.

Therefore, a PHOSITA would have found the limitation recited claim 3 to be obvious based on Kilpatrick and Piccard. EX1003, ¶370. As shown, the Kilpatrick-Piccard combination discloses all elements recited in claim 1 from which claim 3 depends. Accordingly, claim 3 should be found invalid under 35 U.S.C. § 103 based on Kilpatrick and Piccard.

4. Claim 4

The method of claim 3, 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.

Piccard discloses that when malware is identified on a computer, the website identification module of Piccard uses the download history of the web browser to identify the source of the file (corresponding to “the recorded history ...which includes information about files downloaded to the computer and a source of each of the files”). EX1007, ¶¶[0021]-[0022]; EX1003, ¶¶372-374. The '932 patent describes “browser cache” as including a listing of times, URLs, and objects that were downloaded, which a PHOSITA would understand to correspond to the web browser’s history log of Piccard which also stores this information. EX1001, 6:20-35; EX1003, ¶¶375-377.

Therefore, a PHOSITA would have found the limitation recited claim 4 to be obvious based on Piccard. EX1003, ¶¶378-379. As shown, the Kilpatrick-Piccard combination discloses all elements recited in claims 1 and 3 from which claim 4 depends. Accordingly, claim 4 should be found invalid under 35 U.S.C. § 103 based on Kilpatrick and Piccard.

5. Claim 5

a. A system for identifying a source of activity on a computer that is indicative of pestware including:

Kilpatrick and Piccard both teach this preamble. Kilpatrick is directed toward a system that monitors applications for anomalous behavior in order to detect intrusions and processes responsible. EX1008, 1:9-27,4:15-25; EX1003, ¶¶383-385. Piccard teaches a process for protecting a computing device and including operations or methods to determine the source of malware acting on the system (corresponding to “identifying an origin of activity on a computer”). EX1007, ¶¶[0005],[0012],[0019]-[0023]; EX1003, ¶¶386-389.

b. 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;

Kilpatrick teaches a “kernel-loadable module [that] intercepts all system calls as they are made by a program,” which corresponds to “a kernel-level

monitor configured to monitor API call activity.” EX1003, ¶¶392-393; EX1008, 4:33-55. Kilpatrick notes that these intercepts occur in the kernel or at the kernel level. EX1003, ¶¶393-395; EX1008, 4:59-62,12:3-6. A PHOSITA would have understood that these system calls intercepted at the kernel level would include API calls which are calls that allow user-space applications to call into kernel space. EX1003, ¶429 (citing EX1013, p.1). Finally, Kilpatrick teaches that these system calls are stored and viewable in a sliding event window showing recent history of system calls (corresponding to “configured ...to store information related to the API call activity in a log”). EX1003, ¶395; EX1008, 8:33-38.

Therefore, a PHOSITA would have found these limitations to be obvious based on Kilpatrick. EX1003, ¶396.

c. 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;

Kilpatrick teaches that the intercepted system calls are stored in a sliding window log of recent system calls for further analysis. EX1003, ¶¶399-400; EX1008, 8:33-45. Kilpatrick discloses an intrusion detection system (IDS) that analyzes each system call pair that is inserted into the event window based on a distance matrix (corresponding to “heuristics module”) to determine if the sequence is anomalous (corresponding to “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”). EX1003, ¶¶399-404; EX1008, 8:25-40. If the sequence is new, the detect process will measure the magnitude of the difference between several known sequences in the distance matrix and the intercepted system call and compare to a predefined threshold(corresponding to “analyzing, heuristically, computer activity to determine whether one or more weighted factors associated with an activity exceeds a threshold”). EX1003, ¶¶402-403; EX1008, 9:8-23. A PHOSITA would have understood comparing a number of distance values against a predefined threshold by using Kilpatrick’s ‘minimum value’ involves weighting the other values. EX1008, 11:19-28; EX1003, ¶404.

Therefore, a PHOSITA would have found these limitations to be obvious based on Kilpatrick.EX1003, ¶405.

d. a research portion configured to identify, in response to a prompt from the heuristics module, a suspected pestware object on the computer; and

Kilpatrick teaches analyzing stored sequences of system calls to determine if a new system call is an anomalous sequence and could be malware. EX1008, 9:5-25; EX 1003, ¶408. Kilpatrick notes, as explained above, that a system call is associated with a program or process and that each system call of a program can be intercepted. EX1008, 8:33-55; EX 1003, ¶¶399-400. A PHOSITA would have

known it to be possible, and would find it obvious and routine, to identify the executable file from which the process was launched (corresponding to “to identify...a suspected pestware object on the computer”). EX1003, ¶¶71-75,408-409. This executable file would then represent the source of the activity, and a PHOSITA would have understood process ID and file locations / paths to be common convertible identifiers for executable programs. EX1003, ¶¶71-75,409. Kilpatrick discloses that the system call event window is a block of system calls that is analyzed by the IDS if the system call sequence is not recognized by the distance matrix. EX1008, 6:29-65; EX 1003, ¶¶407-409.

Further, Piccard also teaches storing and accessing file download history logs from a web browser in order to identify a web site that was the source of the malicious file. EX1007, pp.2,5; EX1003, ¶¶410-411. A PHOSITA would have been motivated to incorporate the download history log of Piccard via predictable methods into the malicious program detector of Kilpatrick. EX1006, p.5; EX1007, ¶¶[0015],[0017], [0019]; EX1003, ¶¶63-66,409-411 (citing EX1010).

Therefore, a PHOSITA would have found these limitations to be obvious based on Kilpatrick and Piccard. EX1003, ¶¶411-412.

- e. 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**

Piccard teaches a reporting module that reports information (corresponding to “a reporting portion configured to generate a report”) regarding the downloaded file, its source, and other relevant information (e.g., file name) to a remotely-located computer in the computer network of the protected / monitored computer. EX1007, ¶¶[0015]-[0016]; EX1003, ¶¶415-417. The remote computer of Piccard then analyzes the relevant information “to determine whether the file does, in fact, include malware and whether the Web site is, in fact, a malware distribution site.” EX1007, ¶[0023]; EX1003, ¶416. A PHOSITA would understand that this analysis corresponds to “so as to enable the externally networked pestware research entity to research whether the externally networked source is a source of pestware”. EX1003, ¶¶416-417. Therefore, a PHOSITA would have found these limitations obvious based on Piccard. *Id.* at ¶¶417-418.

- f. 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.**

In the combined Kilpatrick-Piccard system that identifies the source of a suspected malicious file, a PHOSITA would have found it obvious to both obtain the identity of the file and to store that identity for future reference, in order to gain

processing efficiency by acquiring the information only once. EX1003, ¶¶71-74,420-422 (citing EX1011 and EX1012). Thereafter, since the stored activity includes the API call and the process identity associated with it. It would have been obvious to a PHOSITA that the identity of the file corresponding to the process can be obtained, such as by storing it alongside the activity in the log, or by looking up the stored file name based on the process ID stored in the activity log. *Id.* Therefore, a PHOSITA would have found these limitations obvious based on Kilpatrick and Piccard. *Id.* at ¶¶421-423.

Therefore, a PHOSITA would have found claim 1 to be obvious based on the Kilpatrick-Piccard combination. Accordingly, claim 1 should be found invalid under 35 U.S.C. § 103 based on Kilpatrick and Piccard.

6. Claim 6

The system of claim 5, wherein the information comprises an identity of at least one process that made at least one API call in the log.

Kilpatrick teaches intercepting system calls associated with a program or process to identify malware. EX1008, 4:25-45. As noted regarding the limitation of claim 1[b], a PHOSITA would have understood that system call sequences are linked to processes (programs / executables) and their process IDs (corresponding to “the information comprises an identity of at least one process that made at least one API call in the log”). EX1003, ¶¶71-74,322 (citing EX1012)(citing EX1011).

Therefore, a PHOSITA would have found the limitation recited claim 6 to be obvious based on Kilpatrick. EX1003, ¶¶425-426. As shown, the Kilpatrick-Piccard combination discloses all elements recited in claim 5 from which claim 6 depends. Accordingly, claim 7 should be found invalid under 35 U.S.C. § 103 based on Kilpatrick and Piccard.

7. Claim 7

The system of claim 5, 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.

Kilpatrick discloses that the IDS transmits information regarding each new system call to the distance matrix (corresponding to “the heuristics module”) which compares the system call to past known pairs to determine whether the new system call relates to an intrusion (corresponding to “the heuristics module is configured to receive information about API call activity from the kernel-level monitor and to determine whether the API call activity is indicative of pestware”). EX1008, 4:25-55; EX1003, ¶428. As described regarding claim limitation 1[b], a PHOSITA would have understood that these system calls intercepted at the kernel level would include API calls which are calls that allow user-space applications to call into kernel space. EX1003, ¶¶428-431; EX1008, 4:25-55.

Therefore, a PHOSITA would have found the limitation recited claim 7 to be obvious based on Kilpatrick. EX1003, ¶432. As shown, the Kilpatrick-Piccard combination discloses all elements recited in claim 5 from which claim 7 depends. Accordingly, claim 7 should be found invalid under 35 U.S.C. § 103 based on Kilpatrick and Piccard.

8. Claim 8

The system of claim 5, wherein the kernel-level monitor is configured to intercept at least one API call.

Kilpatrick teaches a “kernel-loadable module [that] intercepts all system calls as they are made by a program,” which corresponds to “the kernel-level monitor is configured to intercept at least one API call.” EX1003, ¶434; EX1008, 4:33-55. Kilpatrick notes that these intercepts occur in the kernel or at the kernel level. EX1003, ¶¶393-395; EX1008, 4:59-62, 12:3-6. A PHOSITA would have understood that these system calls intercepted at the kernel level would include API calls which are calls that allow user-space applications to call into kernel space. EX1003, ¶¶434-436 (citing EX1013, p.1).

Therefore, a PHOSITA would have found the limitation recited claim 8 to be obvious based on Piccard. EX1003, ¶436. As shown, the Kilpatrick-Piccard combination discloses all elements recited in claim 5 from which claim 8 depends.

Accordingly, claim 8 should be found invalid under 35 U.S.C. § 103 based on Kilpatrick and Piccard.

9. Claim 9

The system of claim 5, 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.

As shown for 1[h], Piccard discloses that the recorded “Web address of the file” can be a web URL or an IP address. EX1003, ¶¶438-439; EX1007, ¶[0013],[0021]. A PHOSITA would have understood that a URL can be converted to an IP address via any domain name system (DNS) server which was readily available at the time. EX1003, ¶440.

Therefore, a PHOSITA would have found the limitation recited claim 7 to be obvious based on Piccard. EX1003, ¶¶181, 440-441. As shown, the Kilpatrick-Piccard combination discloses all elements recited in claim 5 from which claim 9 depends. Accordingly, claim 9 should be found invalid under 35 U.S.C. § 103 based on Kilpatrick and Piccard.

10. Claim 10

The system of claim 5, wherein the research portion is configured to access at least a portion of a recorded history of externally networked sources.

Claim 10 is equivalent to claim 3. As discussed re claim 3, Piccard discloses that when malware is identified on a computer, the website identification module of Piccard uses the download history of the web browser to identify the network source of the file (corresponding to “at least a portion of a recorded history of externally networked sources”). EX1007, ¶¶[0021]-[0022]; EX1003, ¶¶442-444. A PHOSITA would have understood that the web browser’s history log of Piccard stores information that would be in a “browser cache” (e.g., a listing of times, URLs, and objects that were downloaded). EX1003, ¶369. Further, Piccard teaches a reporting information to a remotely-located computer in the computer network of the protected / monitored computer (corresponding to “access[ing] at least a portion of a recorded history of externally networked sources”). EX1007, ¶[0015]; EX1003, ¶¶443-445.

Therefore, a PHOSITA would have found the limitation recited claim 10 to be obvious based on Piccard. EX1003, ¶445. As shown, the Kilpatrick-Piccard combination discloses all elements recited in claim 5 from which claim 9 depends. Accordingly, claim 9 should be found invalid under 35 U.S.C. § 103 based on Kilpatrick and Piccard.

11. Claim 11

The system of claim 10, 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.

The claim 11 limitations are equivalent to limitations in claim 4. As described re claim 4, Piccard discloses that when malware is identified on a computer, the website identification module of Piccard uses the download history of the web browser to identify the source of the file. EX1007, ¶¶[0021]-[0022]; EX1003, ¶¶448-449. The '243 patent describes “browser cache” as including a listing of times, URLs, and objects that were downloaded, which a PHOSITA would understand to correspond to the web browser’s history log of Piccard which also stores this information. EX1001, 6:20-35; EX1003, ¶449.

Therefore, a PHOSITA would have found the limitation recited claim 11 to be obvious based on Piccard. EX1003, ¶¶450-451. As shown, the Kilpatrick-Piccard combination discloses all elements recited in claims 5 and 10 from which claim 11 depends. Accordingly, claim 11 should be found invalid under 35 U.S.C. § 103 based on Kilpatrick and Piccard.

12.Claim 12

- a. 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:**

The preamble of claim 12 is similar to the preamble of claim 1 except that it recites a “non-transitory computer-readable medium including processor-executable instructions for” instead of “method.” As discussed re 1[a], Kilpatrick and Piccard both disclose computer systems and computer-implemented methods of malware detection. A PHOSITA would have known that methods executing on a computer are implemented as executable instructions that load into a processor from a non-transitory tangible computer readable storage medium, such as a hard drive. EX1003, ¶¶454-461. Accordingly, Kilpatrick and Piccard teach the preamble. EX1003, ¶454.

The limitations of claim 12 are otherwise identical to the limitations in claim 1, with a small exception in the final limitation 12[h]. EX1003, ¶463. Therefore, in the analysis of claim 12 reference is made to the corresponding limitation discussions in claim 1.

- b. monitoring, using a kernel-mode driver, API call activity on the computer;**

As shown re 1[b], a PHOSITA would have found this limitation obvious based on Kilpatrick. EX1003, ¶463.

c. storing information related to the API call activity in a log;

As shown re 1[c], a PHOSITA would have found this limitation obvious based on Kilpatrick. EX1003, ¶463.

d. analyzing, heuristically, the API call activity to determine whether one or more weighted factors associated with the API call activity exceeds a threshold;

As shown re 1[d], a PHOSITA would have found this limitation obvious based on Kilpatrick. EX1003, ¶463.

e. identifying, based upon the API call activity, a suspected pestware object on the computer;

As shown re 1[e], a PHOSITA would have found this limitation obvious based on Kilpatrick. EX1003, ¶463.

f. 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

As shown re 1[f], a PHOSITA would have found this limitation obvious based on Kilpatrick and Piccard. EX1003, ¶463.

g. reporting the identity of the externally networked source to an externally networked pestware research entity,

As shown re 1[g], a PHOSITA would have found this limitation obvious based on Piccard. EX1003, ¶463.

h. wherein 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.

As shown re 1[h], Kilpatrick teaches this limitation the addition of the words “selected by an identifier.” EX1003, ¶463. The identifiers listed in 12[h] include a URL. As shown re 1[h], Piccard discloses that the recorded “Web address of the file” can be a web URL or an IP address. EX1003, ¶¶438-439,463; EX1007, ¶¶[0013],[0021]. A PHOSITA would have understood that a URL can be converted to an IP address via any domain name system (DNS) server which was readily available at the time. EX1003, ¶440. Therefore, a PHOSITA would have found these limitations to be obvious based on Kilpatrick and Piccard. EX1003, ¶¶461-464.

Therefore, a PHOSITA would have found claim 12 to be obvious based on the Kilpatrick-Piccard combination. Accordingly, claim 12 should be found invalid under 35 U.S.C. § 103 based on Kilpatrick and Piccard.

13. Claim 13

The non-transitory computer-readable medium of claim 12, wherein the instructions for identifying the suspected pestware object include instructions for accessing an activity log that includes information that relates the activity to the suspected pestware object.

Other than reciting the non-transitory computer-readable medium, claim 13 is essentially identical to claim 2. As shown re claim 2, a PHOSITA would have found the limitation recited claim 13 to be obvious based on Kilpatrick. EX1003, ¶466. As shown, the Kilpatrick-Piccard combination discloses all elements recited in claim 12 from which claim 13 depends. Accordingly, claim 13 should be found invalid under 35 U.S.C. § 103 based on Kilpatrick and Piccard.

14.Claim 14

The non-transitory computer-readable medium of claim 12, wherein the instructions for identifying a reference include instructions for accessing at least a portion of a recorded history of externally networked sources.

Other than reciting the non-transitory computer-readable medium, claim 13 is essentially identical to claim 3. As shown re claim 3, a PHOSITA would have found the limitation recited claim 14 to be obvious based on Piccard. EX1003, ¶468. As shown, the Kilpatrick-Piccard combination discloses all elements recited in claim 12 from which claim 13 depends. Accordingly, claim 13 should be found invalid under 35 U.S.C. § 103 based on Kilpatrick and Piccard.

15. Claim 15

The non-transitory computer-readable medium of claim 14, 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.

Other than reciting the non-transitory computer-readable medium, claim 13 is essentially identical to claim 4. As shown re claim 4, a PHOSITA would have found the limitation recited claim 15 to be obvious based on Kilpatrick or Kilpatrick and Piccard. EX1003, ¶470. As shown, the Kilpatrick-Piccard combination discloses all elements recited in claims 12 and 14 from which claim 15 depends. Accordingly, claim 15 should be found invalid under 35 U.S.C. § 103 based on Kilpatrick and Piccard.

VI. NO BASIS FOR DISCRETIONARY DENIAL

There is no basis to deny institution under 35 U.S.C. §§ 314(a), 325(d).

There is parallel court litigation, so *Fintiv* factors are addressed preliminarily. First, if IPR is instituted, Petitioner stipulates to not raise in the parallel District Court proceedings any ground raised or that could have been reasonably raised in the IPR. *Sotera Wireless, Inc., v. Masimo Corp.*, No. IPR2020-01019, Paper 12 at 19 (P.T.A.B. Dec. 1, 2020) (precedential, designated Dec. 17, 2020). Second, no stay has been entered in the parallel litigation. Third, trial is currently set for August 19, 2024. Trial is currently set for five different

cases on that same date in the same Court against Webroot, of which Trend Micro's case is just one. Trial will not proceed on all five cases on the same date, and it is still unclear which, if any, parties will proceed to trial on that date and when trial would be scheduled for the remaining defendants. Thus, it is unclear the exact date Trend Micro's case will go to trial, and it is possible for this inter partes review to reach final written decision before then. Fourth, it is early in the parallel litigation as the parties are still in fact discovery, which is not set to close until January 18, 2024, after which the parties still have expert discovery, dispositive motions, and pretrial disclosures before reaching trial. Finally, Petitioner and Webroot are parties in the parallel litigation as identified in the Mandatory Notices.

Discretionary denial is strongly disfavored here because the "same or substantially the same art or arguments" were not presented to the Office, and the Office "erred in a manner material" to patentability by not asserting the Abad, Piccard, and Kilpatrick references. *See Advanced Bionics, LLC v. MED-EL Elektromedizinische Gerate GmbH*, IPR2019-01469, Paper 6, 8-9 (Feb. 13, 2020). Analysis of this issue is guided by the "*Becton*" factors. *Id.* at 9-11.

Abad, Piccard, and Kilpatrick were not cited, individually or in combination, in any Office communications. *See* EX1006. Regarding *Becton* factors (a) (material differences between asserted art and prior art) and (b) (cumulative nature of the asserted art and prior art), Abad, Piccard, and Kilpatrick are materially

different from the references asserted in Office communications. Thus, the individual references of Abad, Piccard, and Kilpatrick are not merely cumulative of references the Office relied on. Regarding *Becton* factor (d) (extent of overlap), the arguments in this Petition do not overlap with arguments made during examination. Further, discretionary denial under § 325(d) is still not proper because the Office made a “material error” in not considering the Abad, Piccard, and Kilpatrick references.

Regarding *Becton* factors (c) (evaluation of art during examination), none of Abad, Piccard, and Kilpatrick were used in any claim rejections, weighing strongly against exercising discretion. *See Celco Partnership v. Huawei Device Co.*, IPR2020-01117, Paper 10, 13 (Feb. 3, 2021).

Regarding *Becton* factors (e) (examiner error) and (f) (other facts), this petition specifically points out and explains how Abad, Piccard, and Kilpatrick disclose all limitations of the claims.

VII. CONCLUSION

Inter partes review of claims **1-15** of U.S. Patent No. **8,719,932** is requested based on the grounds described above.

Respectfully submitted,

The Marbury Law Group, PLLC

A handwritten signature in black ink, reading "Robert M. Hansen", written over a horizontal line.

Robert M. Hansen, Reg. No. 43,656
Scott B. Amankwatia, Reg. No. 78,226
Matthew J. Anderson, Reg. No. 78,257

Attorneys for Petitioner

Date: September 7, 2023

The Marbury Law Group, PLLC
11800 Sunrise Valley Drive
15th Floor
Reston, VA 20191
Tel: (703) 391-2900

CERTIFICATION OF SERVICE (37 C.F.R. §§ 42.6(e), 42.105(a))

The undersigned hereby certifies that the above-captioned **PETITION FOR INTER PARTES REVIEW OF U.S. PATENT NO. 8,719,932**, Petitioner's power of attorney, and all associated exhibits were served in their entireties on September 7, 2023, on the following party via Federal Express:

**Sprinkle IP Law Group
1301 W. 25th Street, Suite 400
Austin, TX 78705**

A handwritten signature in black ink, reading "Robert M. Hansen", is written over a horizontal line.

Robert M. Hansen, Reg. No. 43,656
Attorney for Petitioner

Date: September 7, 2023

The Marbury Law Group, PLLC
11800 Sunrise Valley Drive
15th Floor
Reston, VA 20191
Tel: (703)-391-2900

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMITATION

Pursuant to 37 C.F.R. § 42.24 *et seq.*, the undersigned certifies that this Petition complies with the 14,000-word type-volume limitation. The Petition contains **12,524** words, excluding the parts of the Petition exempted.

The Marbury Law Group, PLLC

A handwritten signature in black ink, reading "Robert M. Hansen", written over a horizontal line.

Robert M. Hansen, Reg. 43,656
Attorney for Petitioner

Date: September 7, 2023

THE MARBURY LAW GROUP, ^{PLLC}
11800 Sunrise Valley Drive
15th Floor
Reston, VA 20191
Tel: 703-391-2900