

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

TREND MICRO, INC.
Petitioner

v.

WEBROOT, INC.

Case No. IPR2023-01390
Patent No. 8,201,243

**PETITION FOR INTER PARTES REVIEW
OF U.S. PATENT NO. 8,201,243**

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 '243 Patent.....	5
A. Claim of Priority of the '243 patent	5
B. Specification of the '243 Patent	5
C. Summary of the Prosecution History	6
D. Level of Ordinary Skill in the Art	9
E. Claim Construction.....	9
V. Grounds of Rejection.....	10
A. Ground 1: Claims 1-14 are unpatentable under 35 U.S.C. § 103(a) as obvious in view of Abad and Piccard.....	11
Motivation to Combine Abad and Piccard.....	11
1. Claim 1	13
a. A method for identifying an origin of activity on a computer that is indicative of pestware comprising:.....	13
b. monitoring, using a kernel-mode driver, the computer for activity that is indicative of pestware, wherein the monitoring includes monitoring API calls and storing a history of at least a portion of the API calls in an activity log;	14
c. analyzing, heuristically, computer activity to determine whether one or more weighted factors associated with an activity exceeds a threshold so as to arrive at a determination that the activity is indicative of pestware;	14

d. identifying, based upon the activity, an object residing on the computer that is a suspected pestware object;.....	16
e. accessing, in response to the identifying an object, at least a portion of a recorded history of externally networked sources that the computer received files from so as to identify a reference to an identity of a particular externally networked source tat the suspected pestware object originated from; and	16
f. reporting the identity of the particular externally networked source to an externally networked pestware research entity so as to enable the externally networked pestware research entity to research whether the particular externally networked source is a source of pestware.....	18
2. Claim 2	19
The method of claim 1, wherein the particular externally networked source is identified by an identifier selected from the group consisting of an I.P. address and a URL.	
3. Claim 3	20
The method of claim 2, wherein the identifying includes accessing an activity log that includes information that relates the activity to the suspected pestware object.....	
4. Claim 4	21
The method of claim 1, wherein the recorded history resides in a browser cache, which includes information about files downloaded to the computer and a source of each of the files.	
5. Claim 5	22
The method of claim 1, 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.....	
6. Claim 6	23

a.	A system for identifying a source of activity on a computer that is indicative of pestware including:	23
b.	an activity monitor configured to monitor API calls and to store a history of at least a portion of the API calls in an activity log, wherein the activity monitor includes a kernel-mode driver adapted to intercept the API calls;	24
c.	a heuristics module configured to identify an activity on the computer that is indicative of pestware residing on the computer and to analyze the activity to determine whether one or more weighted factors associated with the activity exceeds a threshold;and	25
d.	a research portion configured to access, in response to a prompt from the heuristics module, a first set of recorded information on the computer that relates the activity to at least one file residing on the computer, and wherein the research portion is onfigured to access a second set of recorded information on the computer that relates the at least one file to an externally networked source from which the file was received; and ..	26
e.	a reporting portion configured to generate a report that identifies the externally networked source of the file and to report an identity of the externally networked source to an externally networked pestware research entity so as to enable the externall networked pestware research entity to research whether the externally networked source is a source of pestware.	28
7.	Claim 7	29
	The system of claim 6, wherein activity monitor is configured to store an identity of each process that made each of the API calls in the stored history, and wherein the activity monitor is configured to store an identity of each file that corresponds to each the processes that made the API calls in the stored history so as to create a relation between each API call and at least one file.	29
8.	Claim 8	31

The system of claim 6, wherein the heuristics module is configured to receive information about the API calls from the activity monitor and determine whether the API calls are indicative of pestware.	31
9. Claim 9	31
The system of claim 6, wherein the first set of recorded information and the second set of recorded information reside in the same log file on a file storage device of the computer.....	31
10. Claim 10	32
The system of claim 6, wherein the externally networked source is identified by an identifier selected from the group consisting of an I.P. address and a URL.....	32
11. Claim 11	33
The system of claim 6 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.....	33
12. Claim 12	33
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:...	33
b. monitoring, with a kernel-mode driver, the computer for activity that is indicative of pestware, wherein the instructions for monitoring include instructions for monitoring API calls and storing a history of at least a portion of the API calls in an actiity log;	34
c. analyzing, heuristically, computer activity to determine whether one or more weighted factors associated with an activity exceeds a threshold so as to arrive at a determination that the activity is indicative of pestware;.....	35

d. identifying, based upon the activity, an object residing on the computer that is a suspected pestware object;.....	35
e. accessing, in response to the identifying an object, at least a portion of a recorded history of externally networked sources that the computer received files from so as to identify a reference to an identity of a particular externally networked source tat the suspected pestware object originated from; and	35
f. reporting the identity of the particular externally networked source to an externally networked pestware research entity so as to enable the externally networked pestware research entity to research whether the particular externally networked source is a source of pestware.....	35
B. Ground 2: Claims 1-14 are unpatentable under 35 U.S.C. § 103 as obvious in view of Kilpatrick (EX1008) and Piccard (EX1006).	37
Motivation to Combine Kilpatrick and Piccard	37
1. Claim 1	39
a. A method for identifying an origin of activity on a computer that is indicative of pestware comprising:.....	39
b. monitoring, using a kernel-mode driver, the computer for activity that is indicative of pestware, wherein the monitoring includes monitoring API calls and storing a history of at least a portion of the API calls in an activity log;	39
c. analyzing, heuristically, computer activity to determine whether one or more weighted factors associated with an activity exceeds a threshold so as to arrive at a determination that the activity is indicative of pestware;.....	40
d. identifying, based upon the activity, an object residing on the computer that is a suspected pestware object;.....	41
e. accessing, in response to the identifying an object, at least a portion of a recorded history of externally networked sources that the computer received files from so as to identify a reference to an identity of a	

particular externally networked source tat the suspected pestware object originated from; and	42
f. reporting the identity of the particular externally networked source to an externally networked pestware research entity so as to enable the externally networked pestware research entity to research whether the particular externally networked source is a source of pestware.....	43
2. Claim 2	44
The method of claim 1, wherein the particular externally networked source is identified by an identifier selected from the group consisting of an I.P. address and a URL.	44
3. Claim 3	45
The method of claim 2, wherein the identifying includes accessing an activity log that includes information that relates the activity to the suspected pestware object.....	45
4. Claim 4	46
The method of claim 1, wherein the recorded history resides in a browser cache, which includes information about files downloaded to the computer and a source of each of the files.	46
5. Claim 5	47
The method of claim 1, 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.....	47
6. Claim 6	48
a. A system for identifying a source of activity on a computer that is indicative of pestware including:	48
b. an activity monitor configured to monitor API calls and to store a history of at least a portion of the API calls in an activity log, wherein the	

activity monitor includes a kernel-mode driver adapted to intercept the API calls;	48
c. a heuristics module configured to identify an activity on the computer that is indicative of pestware residing on the computer and to analyze the activity to determine whether one or more weighted factors associated with the activity exceeds a threshold; and	49
d. a research portion configured to access, in response to a prompt from the heuristics module, a first set of recorded information on the computer that relates the activity to at least one file residing on the computer, and wherein the research portion is onfigured to access a second set of recorded information on the computer that relates the at least one file to an externally networked source from which the file was received; and ..	50
e. a reporting portion configured to generate a report that identifies the externally networked source of the file and to report an identity of the externally networked source to an externally networked pestware research entity so as to enable the externall networked pestware research entity to research whether the externally networked source is a source of pestware.	52
7. Claim 7	53
The system of claim 6, wherein activity monitor is configured to store an identity of each process that made each of the API calls in the stored history, and wherein the activity monitor is configured to store an identity of each file that corresponds to each the processes that made the API calls in the stored history so as to create a relation between each API call and at least one file.	53
8. Claim 8	54
The system of claim 6, wherein the heuristics module is configured to receive information about the API calls from the activity monitor and determine whether the API calls are indicative of pestware.	54
9. Claim 9	55

The system of claim 6, wherein the first set of recorded information and the second set of recorded information reside in the same log file on a file storage device of the computer.....	55
10. Claim 10	56
The system of claim 6, wherein the externally networked source is identified by an identifier selected from the group consisting of an I.P. address and a URL.....	56
11. Claim 11	57
The system of claim 6 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.	57
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, with a kernel-mode driver, the computer for activity that is indicative of pestware, wherein the instructions for monitoring include instructions for monitoring API calls and storing a history of at least a portion of the API calls in an actiity log;	58
c. analyzing, heuristically, computer activity to determine whether one or more weighted factors associated with an activity exceeds a threshold so as to arrive at a determination that the activity is indicative of pestware;	58
d. identifying, based upon the activity, an object residing on the computer that is a suspected pestware object;	59
e. accessing, in response to the identifying an object, at least a portion of a recorded history of externally networked sources that the computer	

received files from so as to identify a reference to an identity of a particular externally networked source tat the suspected pestware object originated from; and 59

f. reporting the identity of the particular externally networked source to an externally networked pestware research entity so as to enable the externally networked pestware research entity to research whether the particular externally networked source is a source of pestware.....59

13. Claim 13 60

The non-transitory computer-readable medium of claim 12, wherein the particular externally networked source is identified by an identifier selected from the group consisting of an I.P. address and a URL. 60

14. Claim 14 60

The non-transitory computer-readable medium of claim 12, 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. 60

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, 8-9 (Feb. 13, 2020)	62
<i>Cellco Partnership v. Huawei Device Co.</i> , IPR2020-01117, Paper 10, 13 (Feb. 3, 2021)	63
<i>General Electric v. Vestas</i> , IPR2018-00928, Paper 9, *16-17 (PTAB Nov. 5, 2018)	11
<i>Graham v. John Deere Co.</i> , 383 U.S. 1 (1966)	11
<i>KSR Int’l Co. v. Teleflex, Inc.</i> , 550 U.S. 398 (2007)	11, 12
<i>Phillips v. AWH Corp.</i> , 415 F.3d 1303 (Fed. Cir. 2005)	10
<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)	10

Statutes

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

Rules

37 C.F.R. § 42.10(a)	2
37 C.F.R. § 42.10(b)	2
37 C.F.R. § 42.100(b)	9
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. 8,201,243 to Boney. (“’243”)
1002	Prosecution History of ’243
1003	Expert Declaration of Dr. Seth Nielson
1004	Curriculum Vitae of A.L. Seth Nielson, Ph.D.
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).
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 Immunology</i> , Communications of the ACM 40(1), (Oct. 1997).
1015	Declaration of Ingrid Hsieh-Yee, Ph.D.

Trend Micro, Inc. (“Petitioner”) petitions for *inter partes* review of claims 1-14 of U.S. Patent No. 8,201,243 to Boney, entitled “BACKWARDS RESEARCHING ACTIVITY INDICATIVE OF PESTWARE” (“the ’243 patent,” EX1001), 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. 8,719,932, which is a continuation of the ’243 patent.

The ’243 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, with an amended complaint listing the ’869 patent filed on September 7, 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, with an amended complaint listing the '869 patent filed on September 7, 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, with an amended complaint listing the '869 patent filed on September 7, 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, with an amended complaint listing the '869 patent filed on September 7, 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 '243 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 ’243 patent. EX1015. Abad was not disclosed to or considered by the Examiner who allowed the ’243 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 ’243 patent. Piccard was not submitted to or considered by the Examiner who allowed the ’243 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 ’243 patent. Kilpatrick was not submitted to or considered by the Examiner who allowed the ’243 patent.

B. Statutory Grounds for Challenge

Petitioner requests review of claims 1-14 on the following grounds:

GROUND 1: Claims 1-14 are unpatentable under pre-AIA 35 U.S.C. § 103(a) as obvious in view of Abad (EX1006) and Piccard (EX1007).

GROUND 2: Claims 1-14 are unpatentable under 35 U.S.C. § 103 as obvious in view of Kilpatrick (EX1008) and Piccard (EX1007).

IV. The '243 Patent

A. Claim of Priority of the '243 patent

The '243 patent, entitled “Backwards researching activity indicative of pestware,” issued on June 12, 2012, from U.S. Patent Application No. 11/408,146, filed April 20, 2006. EX1001, Front Cover.

B. Specification of the '243 Patent

The '243 patent describes a method, system, and apparatus for researching an identity of a source of activity that is indicative of pestware. EX1001, Front Cover, Abstract.

Specifically, claims 1-5 are directed to the method for identifying an origin of activity on a computer that is indicative of pestware that includes monitoring the computer activity (via kernel-mode driver), analyzing computer activity to determine if weighted factors associated with an activity exceeds a threshold, identifying an object residing on the computer, accessing at least a portion of a recorded history, and reporting the identity of the particular externally networked source. EX1001, 10:8-46. Dependent claims 2-5 recite further limitations regarding the particular externally networked source, the identifying step, and the recorded history. *Id.*, 10:31-46.

Claims 6-11 are directed to the system for identifying a source of activity on a computer that is indicative of pestware that includes an activity monitor, a heuristics module, a research portion, and a reporting portion. *Id.*, 10:47-11:29. Dependent claims 7-11 recite further limitations regarding the activity monitor, heuristics module, recorded history, recorded information, and the externally networked source. *Id.*, 10:47-11:29.

Claims 12-14 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 that includes instructions for monitoring, analyzing, identifying, accessing, and reporting steps. *Id.*, 11:30-12:32. Dependent claims 13 and 14 recite further limitations regarding the particular externally networked source and the recorded history. *Id.*, 12:23-32.

C. Summary of the Prosecution History

The application that issued as the '243 patent, 11/408,146, was filed on 4/20/06. EX1002, p.158.

In the non-final Office Action that issued on 2/25/10, all pending claims (1-22) were rejected. Claims 1-22 were rejected under 35 U.S.C. § 103(a) as unpatentable over U.S. Patent Publication 2005/0268112 to Wang *et al.* (“Wang”) in view of U.S. Patent Publication 2004/0024864 to Porras *et al.* (“Porras”). EX1002, p.178. Applicants responded to the non-final Office Action by amending

the independent claims. Specifically, the independent claims were amended to recite “externally networked” and “particular externally networked”. EX1002, pp.160–65. In associated remarks, Applicants argued that Porras is not interested in “an externally networked source suspected of originating an attack...but in the internal network’s user or process session through which the attack is made”. *Id.* p.167. Applicants stated that the other cited references fail to cure the deficiencies of Porras. *Id.*

In the final Office Action, issued 11/10/10, all pending claims were rejected. *Id.*, p.136. Claims 1-22 were rejected under 35 U.S.C. § 103(a) as unpatentable over Wang in view of U.S. Patent Application No. 2007/0168694 to Maddaloni *et al.* (“Maddaloni”). Applicants responded to the final Office Action with a Request for Continued Examination by not amending the claims and arguing that Maddaloni is ineligible prior art pursuant to 35 U.S.C. § 103(c)(1). *Id.* at p.112.

In the non-final Office Action that issued on 5/09/11, all pending claims (1-22) were rejected. Claims 1-22 were rejected under 35 U.S.C. § 103(a) as unpatentable over Wang in view of U.S. Patent No. 7,089,428 to Farley *et al.* (“Farley”). *Id.* at p.85. Applicants responded to the non-final Office Action by amending claim 1 to recite, in part “reporting the identity of the particular externally networked source to an externally networked pestware research entity so as to enable the externally networked pestware research entity to research whether

the particular externally networked source is a source of pestware”, and claim 17 to recite, in part “reporting the identity of the particular web site to an externally networked pestware research entity so as to enable the externally networked pestware research entity to research whether the particular externally networked source is a source of pestware”. *Id.* pp.64-68.

In the Notice of Allowability, issued 2/09/12, the Examiner provided an Examiner’s Amendment previously agreed to by the Applicant in an interview amending claim 1 to recite, in part “monitoring, using a kernel-mode driver...wherein the monitoring includes monitoring API calls and storing a history of at least a portion of the API calls in an activity log; analyzing, heuristically, computer activity to determine whether one or more weighted factors associated with an activity exceeds a threshold so as to arrive at a determination that the activity is indicative of pestware...accessing, in response to the identifying an object.”, and amending claim 17 (now claim 12) to recite, in part “monitoring, with a kernel-mode driver...wherein the instructions for monitoring include instructions for monitoring API calls and storing a history of at least a portion of the API calls in an activity log; analyzing, heuristically, computer activity to determine whether one or more weighted factors associated with an activity exceeds a threshold so as to arrive at a determination that the activity is indicative of pestware...accessing, in

response to the identifying an object”. *Id.* at pp.47-49. The patent subsequently issued.

D. Level of Ordinary Skill in the Art

As established by the Declaration of Dr. Seth Nielson dated 9/7/2023 (EX1003, ¶440), a person having ordinary skill in the art (PHOSITA) at the time of the earliest claimed priority date for the '243 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, ¶96.

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 argues claim terms in asserted patents should be given their plain and ordinary meanings. Likewise, the claim construction order in this parallel litigation in the Western District of Texas construed contested terms in the '243 patent under their plain and ordinary meaning with the exception of “pestware.” EX1005, pp.3. Specifically, the court construed “pestware” to mean

“a trojan, spyware, adware, or malware 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). Should the Board construe “pestware” under its plain and ordinary meaning, the arguments and citations of this petition would equally apply to that broader interpretation.

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 challenged claims.

A. Ground 1: Claims 1-14 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 '243 patent and a more than adequate written rationale is provided to support the combination of Abad and Piccard under *KSR*. 550 U.S. at 418.

Motivation to Combine Abad and Piccard

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.

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, ¶¶120-123. 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 ¶125.

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.” *Id.* at ¶127. 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. *Id.* 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, ¶128.

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, ¶131. For example, Abad says “[p]roblems should be fixed, intruders stopped, and data restored.” EX1006, p.2; EX1003, ¶131. 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, ¶132. 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. *Id.*

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, ¶128. 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, ¶136. 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, ¶137.

Accordingly, a PHOSITA would have found this limitation to be obvious based on Abad. EX1003, ¶¶138-139.

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

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 “the monitoring includes monitoring API calls and storing a history of at least a portion of the API calls in an activity log”. EX1006, p.6; EX1003, ¶142. These system calls are data mined for indicators of malware (corresponding to “monitoring... for activity that is indicative of pestware”) and to enable the monitor to evaluate when new processes are launched. EX1006, pp.5-6; EX1003, ¶¶67-69,142. 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.*

Accordingly, a PHOSITA would have found this limitation to be obvious based on Abad. EX1003, ¶143.

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

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, computer activity ...so as to arrive at a determination that the activity is indicative of pestware”). EX1006, pp.5,8; EX1003, ¶¶146-149. 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, computer activity to determine whether one or more weighted factors associated with an 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, ¶150. In addition, Abad incorporates likelihoods, penalties, sliding windows, and thresholds into this decision making (corresponding to “whether one or more weighted factors associated with an activity exceeds a threshold so as to arrive at a determination that the activity is indicative of pestware”), any of which a PHOSITA would understand to be heuristics. EX1006, p.7; EX1003, ¶¶151-153.

Accordingly, a PHOSITA would have found this limitation to be obvious based on Abad. EX1003, ¶154.

d. identifying, based upon the activity, an object residing on the computer that is a suspected pestware object;

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 activity, ...a suspected pestware object”). EX1006, p.6; EX1003, ¶¶156-158. 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, ¶¶71-74,159 (citing EX1012)(citing EX1011). Accordingly, a PHOSITA would have found processes and executable objects interchangeable for identification purposes (corresponding to “identifying, based upon the activity, an object residing on the computer”). *Id.*

Accordingly, a PHOSITA would have found this limitation to be obvious based on Abad. EX1003, ¶160.

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

Abad teaches a logging architecture, as noted regarding limitation 1[d], that aggregates logs in order to “improve the efficiency of detecting intrusions.” EX1006, pp.3,6; EX1003, ¶¶162-163. A PHOSITA would have understood that log aggregation and correlation was quite common for this reason. EX1003, ¶¶63-66,164 (citing EX1010). 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, ¶¶164-165. 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, ¶¶71-74,91. Accordingly, Abad can link an email or network event to a system call and a process via correlation, which corresponds to “accessing... at least a portion of a recorded history of externally networked sources that the computer received files from so as to identify a reference to an identity of a particular externally networked source”. EX1003, ¶129.

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, ¶¶167-169. Furthermore, Abad teaches correlating multiple types of logs together in its system and recognizes the value of so doing. EX1006, p.3. Abad states: “If all this information can be brought together

it would enable more robust attack detection mechanisms” and “In the bottom-up approach we try to gather relevant information from multiple logs to identify specific attack instances... Once an anomaly is detected in one of the logs, the next step is to examine other logs in the same time period.” A PHOSITA would have found Piccard's logs to be compatible with Abad's correlation and data mining techniques EX1006, p.3. 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(citing EX1010).

Therefore, a PHOSITA would have found these limitations to be obvious based on Abad and Piccard. EX1003, ¶171.

- f. reporting the identity of the particular externally networked source to an externally networked pestware research entity so as to enable the externally networked pestware research entity to research whether the particular externally networked source is a source of pestware.**

Abad teaches that log aggregation and correlation typically takes place at a central point or centralized correlation engine. EX1006, p.3; EX1003, ¶¶173-174. 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 particular externally networked source to an externally networked pestware research entity”). EX1007, ¶[0015]; EX1003, ¶¶176-177. 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, ¶177. A PHOSITA would have found Piccard's logs to be compatible with Abad's correlation and data mining techniques. EX1006, p.3; EX1003, ¶178. 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, ¶¶176-178.

Therefore, a PHOSITA would have found these limitations to be obvious based on Abad and Piccard. EX1003, ¶¶179-180. 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 particular externally networked source is identified by an identifier selected from the group consisting of an I.P. address and a URL.

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 particular externally networked source is identified by an identifier”). EX1007, ¶¶0015]; EX1003, ¶182. Further, Piccard discloses that the recorded web address of the identified source website can be a web URL or IP address (corresponding to “identified by an identifier selected from the group consisting of an I.P. address and a URL”). EX1007, ¶¶0013],[0021]; EX1003, ¶183. 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, ¶184.

Therefore, a PHOSITA would have found the limitation recited claim 2 to be obvious based on Piccard. EX1003, ¶185. 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 2, wherein the identifying 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, ¶187. A PHOSITA

would have understood that system call logs identify the process that made the system call. EX1006, pp.5,6; EX1003, ¶¶187-188. A PHOSITA would have known it to be possible, and would have found it obvious, to identify the file 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, ¶¶189-190.

Therefore, a PHOSITA would have found the limitation recited claim 3 to be obvious based on Abad. EX1003, ¶191. As shown, the Abad-Piccard combination discloses all elements recited in claims 1 and 2 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 1, wherein the recorded history resides in a browser cache, which includes information about files downloaded to the computer and a source of each of the files.

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, ¶¶193-194. 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, ¶¶195-196.

Therefore, a PHOSITA would have found the limitation recited claim 4 to be obvious based on Piccard. EX1003, ¶¶197-198. As shown, the Abad-Piccard combination discloses all elements recited in claim 1 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

The method of claim 1, 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[e], 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, ¶200.

Further, Piccard teaches 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, ¶¶202-204. A PHOSITA would have found Piccard's logs to be compatible with Abad's correlation and data mining techniques.
EX1003, ¶178.

Therefore, a PHOSITA would have found the limitation recited claim 5 to be obvious based on Abad or Abad and Piccard. EX1003, ¶¶ 205-206. As shown, the Abad-Piccard combination discloses all elements recited in claim 1 from which claim 5 depends. Accordingly, claim 5 should be found invalid under 35 U.S.C. § 103 based on Abad and Piccard.

6. Claim 6

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. Abad is directed toward detecting malicious or unwanted behavior on a computer through the correlation of multiple logs. EX1006, pp.1,5; EX1003, ¶209. 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, ¶212.

- b. an activity monitor configured to monitor API calls and to store a history of at least a portion of the API calls in an activity log, wherein the activity monitor includes a kernel-mode driver adapted to intercept the API calls;**

Abad teaches using a system call monitor (corresponding to “activity 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 “configured to monitor API calls and to store a history of at least a portion of the API calls in an activity log”. EX1006, p.6; EX1003, ¶218. 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, ¶¶67-69,218. 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 “the activity monitor includes a kernel-mode driver adapted to intercept the API calls.” EX1006, p.5; EX1003, ¶218.

Therefore, a PHOSITA would have found these limitations to be obvious based on Abad. EX1003, ¶219.

- c. a heuristics module configured to identify an activity on the computer that is indicative of pestware residing on the computer and to analyze the activity to determine whether one or more weighted factors associated with the activity exceeds a threshold; and**

Abad teaches that the core data mining tool (called RIPPER) (corresponding to “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 “a heuristics module configured to identify an activity on the computer”). EX1006, pp.5,8; EX1003, ¶¶222-225. 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 (corresponding to “to analyze the activity to determine whether one or more weighted factors associated with the 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, ¶226. In addition, Abad incorporates likelihoods, penalties, sliding windows, and thresholds into this decision making (corresponding to “whether one or more weighted factors associated with the activity exceeds a threshold”). EX1006, p.7; EX1003, ¶¶227-228.

Therefore, a PHOSITA would have found these limitations to be obvious based on Abad. EX1003, ¶229.

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

Abad teaches a logging architecture (corresponding to “a research portion”) as noted regarding limitation 1[d] that aggregates logs in order to more efficiently detect intrusions. EX1006, pp.3,6; EX1003, ¶¶230-232. A PHOSITA would have understood that log aggregation and correlation for behavior analysis was quite common for this reason. EX1003, ¶¶63-66,76-85,233 (citing EX1010, EX1009, and EX1014). 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, ¶234. 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, ¶¶71-74,235-236. Accordingly, Abad can link an email or network event to a system call and a process via correlation and then to an executable file, which corresponds to “a research portion configured to access, in

response to a prompt from the heuristics module, a first set of recorded information on the computer that relates the activity to at least one file residing on the computer.” *Id.*

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 (corresponding to “the research portion is configured to access a second set of recorded information on the computer that relates the at least one file to an externally networked source from which the file was received”). EX1007, pp.2,5; EX1003, ¶¶236-237. A PHOSITA would have found Piccard's logs to be compatible with Abad's correlation and data mining techniques. EX1003, ¶178. 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, ¶¶63-66,237 (citing EX1010).

Therefore, a PHOSITA would have found these limitations to be obvious based on Abad and Piccard. EX1003, ¶238.

- e. a reporting portion configured to generate a report that identifies the externally networked source of the file and to report an identity of the externally networked source to an externally networked pestware research entity so as to enable the externally networked pestware research entity to research whether the externally networked source is a source of pestware.**

Abad teaches that log aggregation and correlation typically takes place at a central point or centralized correlation engine. EX1006, p.3; EX1003, ¶¶174-175. 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 that identifies the externally networked source of the file and to report an identity of the externally networked source to an externally networked pestware research entity”). EX1007, ¶[0015]; EX1003, ¶¶241-242. 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, ¶¶241-242. A PHOSITA would have found Piccard's logs to be compatible with Abad's correlation and data mining techniques. EX1003, ¶178. 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, ¶243.

Therefore, a PHOSITA would have found these limitations to be obvious based on Abad and Piccard. EX1003, ¶¶244-245. Therefore, a PHOSITA would have found claim 6 to be obvious based on the Abad-Piccard combination. 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 6, wherein activity monitor is configured to store an identity of each process that made each of the API calls in the stored history, and wherein the activity monitor is configured to store an identity of each file that corresponds to each the processes that made the API calls in the stored history so as to create a relation between each API call and at least one file.

Abad teaches tracing system calls to identify malware. EX1006, p.5. As noted regarding the limitation of claim 1[b], a PHOSITA would have understood that system call traces identify processes (programs / executables) and their process IDs (corresponding to “activity monitor is configured to store an identity of each process that made each of the API calls in the stored history”). EX1003, ¶¶71-74,246-247 (citing EX1012)(citing EX1011). 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. *Id.*

Since the Abad-Piccard combination is a logging architecture concerned with identifying network and file download sources for malware, a PHOSITA would have found it obvious to store an identity of each file that corresponds to each the processes that made the API calls in the stored history (e.g., aggregated logs). EX1006, p.5; EX1003, ¶¶246-247. Further, Abad teaches correlating logs so as to identify connections between activity such as network activity and system call activity. EX1006, pp.5-6. Similarly, Piccard discloses the aggregation and comparison across collected website file histories in a single database where, in the Abad-Piccard combination, this network activity log of Abad is enhanced to include file downloads from the log of Piccard (corresponding to “so as to create a relation between each API call and at least one file”). EX1006, pp.5-6; EX1003, ¶¶246-247; EX1007, ¶[0014].

Therefore, a PHOSITA would have found the limitation recited claim 7 to be obvious based on Abad and Piccard. EX1003, ¶247. As shown, the Abad-Piccard combination discloses all elements recited in claim 6 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 6, wherein the heuristics module is configured to receive information about the API calls from the activity monitor and determine whether the API calls are indicative of pestware.

As described regarding the limitations of claim 1[b], Abad teaches a system call monitor called APISpy32 (corresponding to “activity 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 is configured to receive information about the API calls from the activity monitor”). EX1006, pp.5-6; EX1003, ¶¶249-253. Further, as also noted above, Abad teaches that the software module called RIPPER performs data mining on the system call logs and other logs to identify abnormal activity and trace it to a malicious process. *Id.*

Therefore, a PHOSITA would have found the limitation recited claim 8 to be obvious based on Abad and Piccard. EX1003, ¶255. As shown, the Abad-Piccard combination discloses all elements recited in claim 6 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 6, wherein the first set of recorded information and the second set of recorded information reside in the same log file on a file storage device of the computer.

Abad teaches that data aggregation of various logs including a network log and a system call log provide a broader view of the computer system and can identify malware efficiently using these logs. EX1006, pp.5-6; EX1003, ¶¶257. A PHOSITA would have understood that combining activity logs onto a single device was commonplace for efficiency reasons and would have been obvious based on the disclosure of Abad. EX1006, p.3; EX1003, ¶258 (citing EX1010, pp.15-17). A PHOSITA would have found Piccard's logs to be compatible with Abad's correlation and data mining techniques. EX1003, ¶178.

Therefore, a PHOSITA would have found the limitation recited claim 9 to be obvious based on Abad. EX1003, ¶260. As shown, the Abad-Piccard combination discloses all elements recited in claim 6 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 6, wherein the externally networked source is identified by an identifier selected from the group consisting of an I.P. address and a URL.

Claim 10 is essentially identical to claim 2 except implemented on a system. As shown re claim 2, a PHOSITA would have found the limitations recited in claim 10 to be obvious based on Piccard. EX1003, ¶¶261-264. As shown, the Abad-Piccard combination discloses all elements recited in claim 6 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 6 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.

Claim 11 is essentially identical to claim 5. As shown re claim 5, a PHOSITA would have found the limitation recited claim 11 to be obvious based on Abad and Piccard. EX1003, ¶¶ 266-270. As shown, the Abad-Piccard combination discloses all elements recited in claim 6 from which claim 10 depends. Accordingly, claim 10 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 re claim 1[a], Abad and Piccard both disclose computer systems and computer-implemented methods

of malware detection. EX1003, ¶139. A PHOSITA would have known that methods executing on a computer are implemented as executable instructions that loaded into a processor from a non-transitory tangible computer readable storage medium, such as a hard drive. EX1003, ¶¶274-278. Accordingly, Abad and Piccard teach the preamble. EX1003, ¶279.

The limitations of claim 12 are otherwise identical to the limitations in claim 1, with a small exception in the first limitation 12[b]. EX1003, ¶279. Therefore, in the analysis of claim 12 reference is made to the corresponding limitation discussions in claim 1.

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

This limitation differs from claim limitation 1[b] only by including the underlined words in “wherein the instructions for monitoring include instructions for monitoring” consistent with the claim form. As shown re claim limitation 1[b], a PHOSITA would have found this limitation to be obvious based on Abad. EX1003, ¶280.

- c. analyzing, heuristically, computer activity to determine whether one or more weighted factors associated with an activity exceeds a threshold so as to arrive at a determination that the activity is indicative of pestware;**

As shown re claim limitation 1[c], a PHOSITA would have found this limitation to be obvious based on Abad. EX1003, ¶280.

- d. identifying, based upon the activity, an object residing on the computer that is a suspected pestware object;**

As shown re claim limitation 1[d], a PHOSITA would have found this limitation to be obvious based on Abad. EX1003, ¶ 280.

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

As shown re claim limitation 1[e], a PHOSITA would have found this limitation to be obvious based on Abad. EX1003, ¶ 280.

- f. reporting the identity of the particular externally networked source to an externally networked pestware research entity so as to enable the externally networked pestware research entity to research whether the particular externally networked source is a source of pestware.**

As shown re claim limitation 1[f], a PHOSITA would have found this limitation to be obvious based on Abad and Piccard. EX1003, ¶ 280.

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 particular externally networked source is identified by an identifier selected from the group consisting of an I.P. address and a URL.

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 Piccard. EX1003, ¶283. 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 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 14 is essentially identical to claim 5. As shown re claim 5, a PHOSITA would have found the limitation recited claim 14 to be obvious based on Piccard. EX1003,

¶285. 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.

B. Ground 2: Claims 1-14 are unpatentable under 35 U.S.C. § 103 as obvious in view of Kilpatrick (EX1008) and Piccard (EX1006).

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

Motivation to Combine Kilpatrick and Piccard

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, ¶¶287-294; 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, 288-290. 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, 288-290.

Kilpatrick also teaches that various actions may be taken to mitigate the impact of malicious code once it is detected. *Id.* at ¶¶ 112-118, 288-290; 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, 292-293; 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, ¶294; 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, ¶294.

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, ¶¶ 297-301. 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 that is indicative of pestware"). EX1007, ¶¶[0019]-[0023]; EX1003, ¶¶ 297-302.

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

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, the computer for activity that is indicative of pestware." EX1003, ¶¶305-306; EX1008, 4:33-55. Kilpatrick notes that these intercepts occur in the kernel or at the kernel level. EX1003, ¶306; 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, ¶¶307-308. (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 “storing a history of at least a portion of the API calls in an activity log”). EX1003, ¶308; EX1008, 8:33-38.

Therefore, a PHOSITA would have found these limitations to be obvious based on Kilpatrick. EX1003, ¶309.

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

Kilpatrick teaches that the intercepted system calls are stored in a sliding window log of recent system calls for further analysis. EX1003, ¶387; 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, ¶¶312-314; 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, ¶¶313-315; 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, ¶315.

Therefore, a PHOSITA would have found these limitations to be obvious based on Kilpatrick. EX1003, ¶¶316-317.

d. identifying, based upon the activity, an object residing on the computer that is a suspected pestware object;

Kilpatrick teaches intercepting all system calls by a program and tracking running processes via the system calls. EX1003, ¶¶320-321; 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 activity, an object residing on the computer”). EX1003, ¶¶71-75,322. This executable file would then represent the source of the activity (corresponding to “an object residing on the computer that is a suspected pestware object”), and a PHOSITA would have understood process ID and file locations / paths to be common convertible identifiers for executable programs. EX1003, ¶¶71-75,322.

Therefore, a PHOSITA would have found these limitations to be obvious based on Kilpatrick. EX1003, ¶¶323.

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

Piccard teaches a malware detection module and a website identification module. EX1003, ¶¶326-327; 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] (corresponding to “accessing, in response to the identifying an object, at least a portion of a recorded history”). EX1003, ¶¶327-328; EX1007, ¶¶[0014]-[0015].

Piccard also teaches storing and accessing file download history logs (corresponding to “recorded history”) from a web browser in order to identify a web site (corresponding to “a reference to an identity of a particular externally networked source”) that was the source of the malicious file (together corresponding to “accessing, in response to the identifying an object, at least a portion of a recorded history of externally networked sources that the computer received files from so as to identify a reference to an identity of a particular externally networked source that the suspected pestware object originated from”).

EX1007, ¶¶[0014]-[0015]; EX1003, ¶¶326-328. 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, ¶¶63-66,328-329 (citing EX1010).

Accordingly, a PHOSITA would have found this limitation to be obvious based on Kilpatrick and Piccard. EX1003, ¶330.

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

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, ¶333. 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, ¶324. 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, ¶335.

Accordingly, a PHOSITA would have found this limitation to be obvious based on Piccard. EX1003, ¶¶336-337. 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 particular externally networked source is identified by an identifier selected from the group consisting of an I.P. address and a URL.

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 particular externally networked source is identified by an identifier”). EX1007, ¶[0015]; EX1003, ¶339. Further, Piccard discloses that the recorded web address of the identified source website can be a web URL or an IP address (corresponding to “identified by an identifier selected from the group consisting of an I.P. address and a URL”). EX1007, ¶[0013],[0021]; EX1003, ¶340. 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, ¶341.

Therefore, a PHOSITA would have found the limitation recited claim 2 to be obvious based on Piccard. EX1003, ¶342. 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 2, wherein the identifying includes accessing an activity log that includes information that relates the activity to the suspected pestware object.

As explained regarding claim limitation 1[b], Kilpatrick discloses monitoring system calls as they are generated by processes interacting with the operating system. EX1003, ¶¶ 344-345; 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, ¶344; 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, ¶345. 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.

Therefore, a PHOSITA would have found the limitation recited claim 3 to be obvious based on Kilpatrick. EX1003, ¶346. As shown, the Kilpatrick-Piccard combination discloses all elements recited in claims 1 and 2 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 1, wherein the recorded history resides in a browser cache, which includes information about files downloaded to the computer and a source of each of the files.

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, ¶348. 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, ¶¶349-352.

Therefore, a PHOSITA would have found the limitation recited claim 4 to be obvious based on Piccard. EX1003, ¶353. As shown, the Kilpatrick-Piccard combination discloses all elements recited in claim 1 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

The method of claim 1, 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[e], Kilpatrick discloses monitoring system calls as they are generated by processes interacting with the operating system (corresponding to “an activity log”, “an event log”, or “monitoring software logs”). EX1003, ¶355; EX1008, 4:37-55.

Further, Piccard teaches 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, ¶¶356-357.

Therefore, a PHOSITA would have found the limitation recited claim 5 to be obvious based on Kilpatrick or Kilpatrick and Piccard. EX1003, ¶¶ 359-359. As shown, the Kilpatrick-Piccard combination discloses all elements recited in claim 1 from which claim 5 depends. Accordingly, claim 5 should be found invalid under 35 U.S.C. § 103 based on Kilpatrick and Piccard.

6. Claim 6

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, ¶¶ 363-365. 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, ¶¶ 366-367.

Therefore, a PHOSITA would have found this limitation to be obvious based on Kilpatrick and Picard. EX1003, ¶369.

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

Kilpatrick teaches a “kernel-loadable module [that] intercepts all system calls as they are made by a program,” which corresponds to “an activity monitor configured to monitor API calls.” EX1003, ¶¶372-373; EX1008, 4:33-55.

Kilpatrick notes that these intercepts occur in the kernel or at the kernel level (corresponding to “the activity monitor includes a kernel-mode driver adapted to intercept the API calls”). EX1003, ¶¶372-374; 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 “configured to monitor API calls”).

EX1003, ¶¶307, 345 (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 a history of at least a portion of the API calls in an activity log”). EX1003, ¶374; EX1008, 8:33-38.

Therefore, a PHOSITA would have found this limitation to be obvious based on Kilpatrick. EX1003, ¶375.

- c. a heuristics module configured to identify an activity on the computer that is indicative of pestware residing on the computer and to analyze the activity to determine whether one or more weighted factors associated with the activity exceeds a threshold; and**

Kilpatrick teaches that the intercepted system calls are stored in a sliding window log of recent system calls for further analysis. EX1003, ¶387; 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 identify an activity on the computer that is indicative of pestware residing on the computer”). EX1003, ¶¶379-380; 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 “to analyze the activity to determine whether one or more weighted factors associated with the activity exceeds a threshold”). EX1003, ¶¶381-383; 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, ¶¶382-383.

Therefore, a PHOSITA would have found this limitation to be obvious based on Kilpatrick. EX1003, ¶384.

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

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, ¶¶387-389. 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, ¶¶113-114, 308. A PHOSITA would have known it to be possible, and would found it obvious and routine, to identify

the executable file from which the process was launched (corresponding to “a first set of recorded information on the computer that relates the activity to at least one file residing on the computer”). EX1003, ¶¶71-75,388. 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, ¶¶71-75,388. 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 (corresponding to “a research portion configured to access, in response to a prompt from the heuristics module, a first set of recorded information”). EX1008, 6:29-65; EX 1003, ¶¶386-388.

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 (corresponding to “the research portion is configured to access a second set of recorded information on the computer that relates the at least one file to an externally networked source from which the file was received”). EX1007, pp.2,5; EX1003, ¶389. 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, ¶¶63-66,390 (citing EX1010).

Therefore, a PHOSITA would have found this limitation to be obvious based on Kilpatrick and Piccard. EX1003, ¶391.

- e. a reporting portion configured to generate a report that identifies the externally networked source of the file and to report an identity of the externally networked source to an externally networked pestware research entity so as to enable the externally networked pestware research entity to research whether the externally networked source is a source of pestware.**

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 “a report that identifies the externally networked source of the file and to report an identity of the externally networked source to an externally networked pestware research entity”). EX1007, ¶¶[0015]-[0016]; EX1003, ¶¶393-395. 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, ¶395. 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, ¶¶395-396.

Therefore, a PHOSITA would have found this limitation to be obvious based on Piccard. EX1003, ¶397. 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.

7. Claim 7

The system of claim 6, wherein activity monitor is configured to store an identity of each process that made each of the API calls in the stored history, and wherein the activity monitor is configured to store an identity of each file that corresponds to each the processes that made the API calls in the stored history so as to create a relation between each API call and at least one file.

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 “activity monitor is configured to store an identity of each process that made each of the API calls in the stored history”). EX1003, ¶¶71-74,399 (citing EX1012)(citing EX1011). 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 (corresponding to “so as to create a relation between each API call and at least one file”). *Id.*

In the combined Kilpatrick-Piccard system, in which a PHOSITA is motivated to identify the source of the suspected malicious file, it would have been obvious to both obtain the identity of the file associated with the suspicious process and to store both for future reference (corresponding to “the activity monitor is configured to store an identity of each file that corresponds to each the processes that made the API calls in the stored history”), in order to gain processing efficiency by acquiring the information only once. EX1007, ¶¶[0006]-[0007]; EX1003, ¶¶71-74,399 (citing EX1012)(citing EX1011).

Therefore, a PHOSITA would have found the limitation recited claim 7 to be obvious based on Kilpatrick and Piccard. EX1003, ¶400. As shown, the Kilpatrick-Piccard combination discloses all elements recited in claim 6 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 6, wherein the heuristics module is configured to receive information about the API calls from the activity monitor and determine whether the API calls are indicative of pestware.

As explained regarding claim limitation 6[c], 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 the [] calls from the activity monitor and determine whether the [] calls are indicative of pestware”). EX1008, 4:25-55; EX1003, ¶¶402-404. 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, ¶¶402-405; EX1008, 4:25-55.

Therefore, a PHOSITA would have found the limitation recited claim 8 to be obvious based on Kilpatrick. EX1003, ¶406. As shown, the Kilpatrick-Piccard combination discloses all elements recited in claim 6 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 6, wherein the first set of recorded information and the second set of recorded information reside in the same log file on a file storage device of the computer.

In the combined Kilpatrick-Piccard system, Kilpatrick intercepts and logs system calls that are associated with a program or process and Piccard logs file downloads and web sites accessed by a program. EX1008, 4:25-55; EX1007, ¶¶[0021]-[0022]; EX1003, ¶¶372-304. A PHOSITA would have understood the value of storing various sets of logging, access history, or file download

information (e.g., the claimed “recorded information”) within a common file or database on a computer, and it was commonly practiced in the art. EX1003, ¶408. A PHOSITA implementing the combination would have been motivated by the benefits enumerated by Rinnan to store these sets of information together, perhaps in a normalized form such as “a process that breaks an event into its component parts and places them into individual database fields.” EX1010, p.16; EX1003, ¶409.

Therefore, a PHOSITA would have found the limitation recited claim 9 to be obvious based on Kilpatrick and Piccard. EX1003, ¶¶ 410-411. As shown, the Kilpatrick-Piccard combination discloses all elements recited in claim 6 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 6, wherein the externally networked source is identified by an identifier selected from the group consisting of an I.P. address and a URL.

Claim 10 is essentially identical to claim 2 except implemented on a system. As shown re claim 2, a PHOSITA would have found the limitations recited in claim 10 to be obvious based on Piccard. EX1003, ¶¶ 413-416. As shown, the Kilpatrick-Piccard combination discloses all elements recited in claim 6 from

which claim 10 depends. Accordingly, claim 10 should be found invalid under 35 U.S.C. § 103 based on Kilpatrick and Piccard.

11. Claim 11

The system of claim 6 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.

Claim 11 is essentially identical to claim 5. As shown re claim 5, a PHOSITA would have found the limitation recited claim 11 to be obvious based on Kilpatrick and Piccard. EX1003, ¶¶ 418-421. As shown, the Kilpatrick-Piccard combination discloses all elements recited in claim 6 from which claim 10 depends. Accordingly, claim 10 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 claim limitation 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 loaded into a processor from a non-transitory tangible computer readable storage medium, such as a hard drive. EX1003, ¶¶ 424-432. Accordingly, Kilpatrick and Piccard teach the preamble. EX1003, ¶433.

The limitations of claim 12 are otherwise identical to the limitations in claim 1, with a small exception in the first limitation 12[b]. EX1003, ¶433. Therefore, in the analysis of claim 12 reference is made to the corresponding limitation discussions in claim 1.

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

This limitation differs from 1[b] only by including the underlined words in “wherein the instructions for monitoring include instructions for monitoring” consistent with the claim form. As shown re 1[b], a PHOSITA would have found this limitation to be obvious based on Kilpatrick. EX1003, ¶433.

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

As shown re 1[c], a PHOSITA would have found this limitation to be obvious based on Kilpatrick. EX1003, ¶433.

d. identifying, based upon the activity, an object residing on the computer that is a suspected pestware object;

As shown re 1[d], a PHOSITA would have found this limitation to be obvious based on Kilpatrick. EX1003, ¶433.

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

As shown re 1[e], a PHOSITA would have found this limitation to be obvious based on Kilpatrick. EX1003, ¶ 433.

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

As shown re 1[f], the combination of Kilpatrick and Piccard renders this limitation obvious. EX1003, ¶ 433.

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 particular externally networked source is identified by an identifier selected from the group consisting of an I.P. address and a URL.

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 Piccard. EX1003, ¶436. 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 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 14 is essentially identical to claim 5. As shown re claim 5, a PHOSITA would have found the limitation recited claim 14 to be obvious based on both Kilpatrick and Piccard. EX1003, ¶438. As shown, the Kilpatrick-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 Kilpatrick and Piccard.

VI. NO BASIS FOR DISCRETIONARY DENIAL

There is no basis to deny institution under 35 U.S.C. § 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. *Advanced Bionics* at 9-11.

Abad, Piccard, and Kilpatrick were not cited, individually or in combination, in any of the office communications. *See* Ex. 1006. 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 combination of references asserted in Office communications because Abad, Piccard, and Kilpatrick disclose the independent claim limitations that the data received from remote devices includes information about the behavior of the object and the mask is generated based on normal behavior of the object determined from the received data including behavior information. Thus, the individual references of Abad, Piccard, and Kilpatrick not merely cumulative of references the Office relied. Regarding *Becton* factor (d) (extent of overlap), the arguments made in *supra* do not overlap with the arguments made during examination.

Even if the Board finds that the “same or substantially the same” art or arguments were presented to the Office, discretionary denial under § 325(d) is still not proper because the Office has made a “material error” in lieu of 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* factor (e) (examiner error) and (f) (other facts), this petition specifically points out and explains how Abad, Piccard, and Kilpatrick discloses all limitations of the claims.

VII. CONCLUSION

Inter partes review of claims 1-14 of U.S. Patent No. 8,201,243 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. 8,201,243**, Petitioner's power of attorney, and all associated exhibits were served in their entireties on September 7, 2023, on the following party via Express Mail:

**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

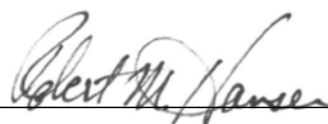
Date: September 7, 2023

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 **13,043** words, excluding the parts of the Petition exempted.

The Marbury Law Group, PLLC

A handwritten signature in dark ink, appearing to read "Robert M. Hansen", is 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