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

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

PETITION FOR INTER PARTES REVIEW OF U.S. PATENT NO. 8,181,244

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

TABLE OF CONTENTS

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

PAYMENT OF FEES.....3

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

Petitioner requests review of claims 1-30 on the following grounds: 4

IV. The '250 Patent 5

A. Claim of Priority of the '250 patent.....5

B. Specification of the '250 Patent.....5

C. Summary of the Prosecution History 6

D. Level of Ordinary Skill in the Art.....9

V. Grounds of Rejection.....10

A. Ground 1: Claims 1-6, 12-18, and 24 are unpatentable under 35 U.S.C. § 103(a) as obvious in view of Halperin and Inoue. 10

1. Claim 1.....13

a. A method of classifying a computer object as malware, the method comprising: ..... Error! Bookmark not defined.

b. at a base computer, receiving data about a computer object from each of plural remote computers on which the object or similar objects are stored, the data including information about the behaviour of the object running on one or more remote computers; .... Error! Bookmark not defined.

c. determining in the base computer whether the data about the computer object received from the plural computers indicates that the computer object is malware; ..... Error! Bookmark not defined.

d. classifying the computer object as malware when the data indicates that the computer object is malware; ..... Error! Bookmark not defined.

e. when the determining does not indicate that the computer object is malware, initially classifying the computer object as not malware; . Error! Bookmark not defined.

f. automatically generating a mask for the computer object that defines acceptable behaviour for the computer object, wherein the mask is generated in accordance with normal behaviour of the object determined from said received data; ..... Error! Bookmark not defined.

g. running said object on at least one of the remote computers; ..... Error! Bookmark not defined.

h. automatically monitoring operation of the object on the at least one of the remote computers; ..... Error! Bookmark not defined.

i. allowing the computer object to continue to run when behaviour of the computer object is permitted by the mask; ..... Error! Bookmark not defined.

j. disallowing the computer object to run when the actual monitored behaviour of the computer object extends beyond that permitted by the mask; and, ... Error! Bookmark not defined.

k. reclassifying the computer object as malware when the actual monitored behaviour extends beyond that permitted by the mask... Error! Bookmark not defined.

2. Claim 2.....19

A method according to claim 1, wherein the data about the computer object that is sent from the plural remote computers to the base computer includes one or more of: executable instructions contained within or constituted by the object; the size of the object; the current name of the object; the physical and folder location of the object on disk; the original name of the object; the creation and modification dates of the object; vendor, product and version and any other information

stored within the object; the object header or header held by the remote computer; and, events initiated by or involving the object when the object is created, configured or runs on the respective remote computers. ..... Error! Bookmark not defined.

3. Claim 3.....21

A method according to claim 1, wherein determining identifies relationships between the object and other objects..... Error! Bookmark not defined.

4. Claim 4.....22

A method according to claim 3, wherein if at least one other object to which said object is related is classed as malware, then classifying said object as malware. ..... Error! Bookmark not defined.

5. Claim 5.....24

A method according to claim 3, wherein said other objects include the object or similar objects stored on at least some of the remote computers. ..... Error! Bookmark not defined.

6. Claim 6.....24

A method according to claim 3, wherein said other objects include other objects that are parent objects or child objects or otherwise process-related objects to said object. ..... Error! Bookmark not defined.

7. Claim 12.....25

A method according to claim 1, comprising if the monitored behaviour of the object running on the remote computer exhibits non-permitted behaviour that extends beyond that permitted by the mask, comparing at the base computer the non-permitted behaviour with the behaviour of other objects and if said behaviour is known to be not malicious for said other objects, allowing said behaviour for the object and modifying the mask to allow that behaviour for that object in future..... Error! Bookmark not defined.

8. Claim 13.....26

a. Apparatus for classifying a computer object as malware, the apparatus comprising: ..... Error! Bookmark not defined.

b. a base computer constructed and arranged to receive data about a computer object from each of plural remote computers on which the object or similar objects are stored, the data including information about the behaviour of the object running on one or more remote computers; ..... Error! Bookmark not defined.

c. the base computer being constructed and arranged to determine whether the data about the computer object received from said plural computers indicates that the computer object is malware; and, ... Error! Bookmark not defined.

d. the base computer being constructed and arranged to classify the computer object as malware when the base computer determines that the data indicates that the computer object is malware, .. Error! Bookmark not defined.

e. wherein the base computer is constructed and arranged to automatically generate a mask for an object that is initially classed not as malware, said mask defining acceptable behaviour for the object built in accordance with normal behaviour of the object determined from said received data, ... Error! Bookmark not defined.

f. wherein operation of the object is automatically monitored when the object is running on at least one of the remote computers, the object being allowed to continue to run when behaviour of the object is permitted by the mask, the object not being permitted to run when the actual monitored behaviour of the object extends beyond that permitted by the mask, and the object is reclassified as malware when the actual monitored behaviour extends beyond that permitted by the mask... Error! Bookmark not defined.

9. Claim 14.....27

Apparatus according to claim 13, the data includes one or more of: executable instructions contained within or constituted by the object; the

size of the object; the current name of the object; the physical and folder location of the object on disk; the original name of the object; the creation and modification dates of the object; vendor, product and version and any other information stored within the object; the object header or header held by the remote computer; and, events initiated by or involving the object when the object is created, configured or runs on the respective remote computers..... Error! Bookmark not defined.

10. Claim 15..... Error! Bookmark not defined.

Apparatus according to claim 13, wherein the base computer is constructed and arranged so that the determining identifies relationships between the object and other objects..... Error! Bookmark not defined.

11. Claim 16..... Error! Bookmark not defined.

Apparatus according to claim 15, the base computer is constructed and arranged so that if at least one other object to which said object is related is classed as malware, then said object is classified as malware. ..... Error! Bookmark not defined.

12. Claim 17..... Error! Bookmark not defined.

Apparatus according to claim 15, wherein the base computer is constructed and arranged wherein the base computer is constructed and arranged so that said other objects include the object or similar objects stored on at least sonic [sic] of said remote computers..... Error! Bookmark not defined.

13. Claim 18..... Error! Bookmark not defined.

Apparatus according to claim 15, wherein the base computer is constructed and arranged so that said other objects include other objects that are parent objects or child objects or otherwise process-related objects to said object. ..... Error! Bookmark not defined.

14. Claim 24..... Error! Bookmark not defined.

A method according to claim 13, wherein, if the monitored behaviour of the object running on the remote computer exhibits non-permitted

behaviour that extends beyond that permitted by the mask, the base computer is arranged to compare the non-permitted behaviour with the behaviour of other objects and if said behaviour is known to be not malicious for said other objects the base computer is arranged to allow said behaviour for the object and to modify the mask to allow that behaviour for that object in future. ..... Error! Bookmark not defined.

B. Ground 2: Claims 7-13, 19-23, and 25-30 are unpatentable under 35 U.S.C. § 103 as obvious in view of Halperin, Inoue, and Patil. 36

1. Claim 7..... Error! Bookmark not defined.

A method according to claim 1, wherein the data is sent in the form of key that is obtained by a hashing process carried out in respect of the objects on the respective remote computers. . Error! Bookmark not defined.

2. Claim 8..... Error! Bookmark not defined.

A method according to claim 7, wherein the key has at least one component that represents executable instructions contained within or constituted by the object. ..... Error! Bookmark not defined.

3. Claim 9..... Error! Bookmark not defined.

A method according to claim 7, wherein the key has at least one component that represents data about said object..... Error! Bookmark not defined.

4. Claim 10..... Error! Bookmark not defined.

A method according to claim 9, wherein said data about said object includes at least one of: the current name of the object; the physical and folder location of the object on disk; the original name of the object; the creation and modification dates of the object; vendor, product and version and any other information stored within the object; the object header or header held by the remote computer; and, events initiated by or involving the object when the object is created, configured or runs on the respective remote computers..... Error! Bookmark not defined.

5. Claim 11..... Error! Bookmark not defined.

A method according to claim 7, wherein the key has at least one component that represents the physical size of the object..... Error! Bookmark not defined.

6. **Claim 19.....**Error! Bookmark not defined.

Apparatus according to claim 13, wherein the base computer is constructed and arranged so as to be able to process data that is sent in the form of key that is obtained by a hashing process carried out in respect of the objects on said respective remote computers..... Error! Bookmark not defined.

7. **Claim 20.....**Error! Bookmark not defined.

Apparatus according to claim 19, wherein the key has at least one component that represents executable instructions contained within or constituted by the object. ..... Error! Bookmark not defined.

8. **Claim 21.....**Error! Bookmark not defined.

Apparatus according to claim 19, wherein the key has at least one component that represents data about said object..... Error! Bookmark not defined.

9. **Claim 22.....**Error! Bookmark not defined.

Apparatus according to claim 21, wherein said data about said object includes at least one of: the current name of the object; the physical and folder location of the object on disk; the original name of the object; the creation and modification dates of the object; vendor, product and version and any other information stored within the object; the object header or header held by the remote computer; and, events initiated by or involving the object when the object is created, configured or runs on the respective remote computers..... Error! Bookmark not defined.

10. **Claim 23.....**Error! Bookmark not defined.

Apparatus according to claim 19, wherein the key has at least one component that represents the physical size of the object..... Error! Bookmark not defined.

11. Claim 25..... Error! Bookmark not defined.

a. A method of providing data about a computer object from a remote computer to a base computer so that a comparison can be made at the base computer with similar data received from other remote computers, the method comprising: ..... Error! Bookmark not defined.

b. providing from a remote computer to a base computer data about a computer object that is stored on the remote computer; . Error! Bookmark not defined.

c. the data including information about the behaviour of the object running on one or more remote computers and including one or more of: executable instructions contained within or constituted by the object; the size of the object; the current name of the object; the physical and folder location of the object on disk; the original name of the object; the creation and modification dates of the object; vendor, product and version and any other information stored within the object; the object header or header held by the remote computer; and, events initiated by or involving the object when the object is created, configured or runs on the respective remote computers; ..... Error! Bookmark not defined.

d. the data being sent in the form of key that is obtained by a hashing process carried out in respect of the object on the remote computer;
Error! Bookmark not defined.

e. automatically generating a mask for the computer object, the mask defining acceptable behaviour for the object built in accordance with normal behaviour of the object determined from said received data;
Error! Bookmark not defined.

f. executing the computer object at the remote computer;..... Error! Bookmark not defined.

g. automatically monitoring operation of the computer object at the remote computer compared to the behaviour permitted by the mask;
Error! Bookmark not defined.

h. allowing the object to continue to run when behaviour of the computer object is permitted by the mask; ... Error! Bookmark not defined.

i. disallowing the object to run when the actual monitored behaviour of the object extends beyond that permitted by the mask; and, ... Error! Bookmark not defined.

j. reclassifying the object as malware when the actual monitored behaviour extends beyond that permitted by the mask, wherein the base computer is arranged to receive information about the behaviour of the object running on one or more remote computers, wherein the step of generating a mask for that object comprises building the mask with the base computer in accordance with normal behaviour of the object determined from said received information. . Error! Bookmark not defined.

12. Claim 26..... Error! Bookmark not defined.

A method according to claim 25, wherein the key has at least one component that represents executable instructions contained within or constituted by the object. ..... Error! Bookmark not defined.

13. Claim 27..... Error! Bookmark not defined.

A method according to claim 25, wherein the key has at least one component that represents data about said object..... Error! Bookmark not defined.

14. Claim 28..... Error! Bookmark not defined.

A method according to claim 27, wherein said data about said object includes at least one of: the current name of the object; the physical and folder location of the object on disk; the original name of the object; the creation and modification dates of the object; vendor, product and version and any other information stored within the object; the object header or header held by the remote computer; and, events initiated by or involving the object when the object is created, configured or runs on the respective remote computers..... Error! Bookmark not defined.

15. Claim 29..... Error! Bookmark not defined.

A method according to claim 25, wherein the key has at least one component that represents the physical size of the object..... Error! Bookmark not defined.

16. Claim 30..... Error! Bookmark not defined.

A non-transitory storage medium storing a computer program comprising program instructions for causing a computer to perform the method of claim 25..... Error! Bookmark not defined.

C. Ground 3: ..... Error! Bookmark not defined.

VI. CONCLUSION 72

TABLE OF AUTHORITIES

Cases

Advanced Bionics, LLC v. MED-EL Elektromedizinische Gerate GmbH,
IPR2019-01469, Paper 6 (Feb. 13, 2020) 72

Cellco Partnership v. Huawei Device Co., IPR2020-01117, Paper 10 (Feb. 3, 2021) 72

General Electric v. Vestas, IPR2018-00928, Paper 9, *16-17 (PTAB Nov. 5, 2018)..... 11

Graham v. John Deere Co., 383 U.S. 1 (1966) 11, 12

KSR Int'l Co. v. Teleflex, Inc., 550 U.S. 398 (2007)..... 11, 12

Phillips v. AWH Corp., 415 F.3d 1303 (Fed. Cir. 2005) (en banc) 10

Sotera Wireless, Inc., v. Masimo Corp.,
No. IPR2020-01019, Paper 12 at 19 (P.T.A.B. Dec. 1, 2020)..... 71

Western Digital Corporation v. Spex Technologies, Inc.,
IPR2018-00084, Paper 14, *11 (PTAB Apr. 25, 2018)..... 10

Statutes

35 U.S.C. § 103..... 4
35 U.S.C. § 325(d) 69, 71
35 U.S.C. §§ 314(a) 69

Rules

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

EXHIBIT LIST

Exhibit No.	Description
1001	U.S. Patent No. 8,719,932 to Boney.
1002	Prosecution History of '932.
1003	Expert Declaration of Dr. Seth Nielson.
1004	Curriculum Vitae of Dr. Seth Nielson.
1005	Webroot, Inc. and Open Text, Inc. v. Trend Micro Inc., Case No. 6:22-cv-00243-ADA-DTG, Claim Construction Order, Dkt. 391 (W.D. Tex., July 25, 2023).
1006	Cristina Abad, *Log Correlation for Intrusion Detection: A Proof of Concept*, 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 *et al*.
1009	Ed Skoudis, *Malware: Fighting Malicious Code,* Pearson (Nov. 2003).
1010	Robert Rinnan, *Benefits of Centralized Log File Correlation*, Gjøvik University College (2005).
1011	Platform SDK: Windows Management Instrumentation, *Win32_Process*, Win32_Process class [WMI] (archive.org) (Jul. 17, 2004).
1012	Matthew M. Lavy, *Windows Management Instrumentation (WMI)*, Sams (Oct. 2001).
1013	Yariv Kaplan, *API Spying Techniques for Windows 9x, NT and 2000*, API Spying Techniques for Windows 9x, NT and 2000 (archive.org) (Feb. 10, 2003).
1014	Stephanie Forrest, *Computer Immunolgy*, Communications of the ACM 40(1), (Oct. 1997).

1015	**Declaration of Ingrid Hsieh-Yee, Ph.D.**

Trend Micro America, Inc. and Trend Micro, Inc. (collectively "Petitioner") petitions for *inter partes* review of claims 1-16 of U.S. Patent No. 8,181,244 to Boney, entitled "Backward researching time stamped events to find an origin of pestware" ("the '244 patent," Ex. 1001), which according to PTO records, is assigned to Webroot, Inc.

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

REAL PARTY IN INTEREST:

The real parties-in-interest are Trend Micro America, Inc. and Trend Micro, Inc.

RELATED MATTERS:

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

The '244 patent is at issue in the following district court litigations:

- *Webroot, Inc. and Open Text, Inc. v. Trend Micro Inc.*, Case No. 6:22-cv-00239 (W.D. Tex.), which was originally filed on March 4, 2022.
- *Webroot, Inc. and Open Text, Inc. v. Sophos LTD.*, Case No. 6:22-cv-00240 (W.D. Tex.), which was originally filed on March 4, 2022.
- *Webroot, Inc. and Open Text, Inc. v. Crowdstrike, Inc. and Crowdstrike Holdings, Inc.*, Case No. 6:22-cv-00241 (W.D. Tex.), which was originally filed on March 4, 2022.

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

LEAD AND BACKUP COUNSEL:

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

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

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

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

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

SERVICE INFORMATION:

Petitioner provides the following service information for designated counsel:

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

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

rhansen@marburylaw.com;

samankwatia@marburylaw.com;

manderson@marburylaw.com; and

pat-docketing@marburylaw.com.

PAYMENT OF FEES

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

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

Petitioner certifies that the '244 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:

Kevin Chen, ECF – Event Correlation for Forensics, Australian Computer, Network & Information Forensics Conference (2003) ("Chen," Ex. 1006) is prior art under pre-AIA § 102(a) because it was published and publicly accessible by June 23, 2005, before the earliest priority date of the '244 patent. EX1009, p.21. Chen was not submitted to or considered by the Examiner who allowed the '244 patent.

U.S. Patent Application Publication No. 2007/0006310 to Piccard, January 4, 2007 ("Piccard," Ex. 1007) is prior art under pre-AIA § 102(e) because the application that published as Piccard was filed June 30, 2005, before the earliest

priority date of the '244 patent. EX1007, Front Cover. Piccard was not disclosed to or considered by the Examiner who allowed the '244 patent.

Zhenmin Li, UCLog: A Unified, Correlated Logging Architecture for Intrusion Detection, Int'l Conf. on Telecomm. Sys.- Modelling & Analysis (2004), ("Li," EX1008) is prior art under pre-AIA § 102(a) because it was published and publicly available no later than May 2005, before the earliest priority date of the '244 patent. EX1009, p. 28. Li was not disclosed to or considered by the Examiner who allowed the '244 patent.

B. Statutory Grounds for Challenge

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

GROUND 1: Claims 1-16 are unpatentable under 35 U.S.C. § 103 as obvious in view of Li (EX1008) and Piccard (EX1007).

GROUND 2: Claims 1-16 is unpatentable under pre-AIA 35 U.S.C. § 103(a) as obvious in view of Chen (EX1006) and Piccard (EX1007).

IV. The ’244 Patent

A. Claim of Priority of the ’244 patent

The ’244 patent, entitled “Backward researching time stamped events to find an origin of pestware,” issued on 5/5/12, from U.S. Patent Application No. 11/408,145, filed 4/20/06. Ex.1001, Front Cover.

B. Specification of the ’244 Patent

The ’244 patent describes methods and systems for identifying an origin of suspected pestware activity on a computer**.** Ex. 1001, 10:8-63.

Specifically, claims 1-8 are directed to the method for identifying an origin of suspected pestware activity on a computer that includes monitoring activity on the computer, generating an activity log, receiving a time of interest, issuing a timestamp, identifying indicia of pestware, accessing a reference, and the recorded history of externally networked sources is stored on the file storage device. Ex. 1001, 10:8-30. Dependent claims 2-8 recite further limitations regarding the steps of the above-mentioned method. Ex. 1001, 10:31-61.

Claims 9-16 are directed to the system for identifying a source of suspected pestware on a computer that includes a hardware processor, a file storage device, a timestamp module, a research portion, a kernel-mode driver, and a reporting portion. Ex. 1001, 10:62-12:26. Dependent claims 10-16 recite further limitations

regarding a log, a heuristics module, the timestamp module, and at least one externally networked source of potential pestware activity**.** Ex. 1001, 11:18-12:26.

C. Summary of the Prosecution History

The application that issued as the '244 patent, U.S. Patent Application No. 11/408,145, was filed on 4/20/06. Ex. 1001, Cover Page.

Prosecution began with a non-final Office Action dated 6/22/09**.** The final round of rejections and amendments is illustrative of the Examiner's findings during prosecution.

In the non-final Office Action that issued on 6/22/09, claims 1-23 were rejected. Claims 1-23 were rejected under 35 U.S.C. § 103(a) as unpatentable over U.S. Patent Application No. 2004/0024864 to Porras *et al*. ("Porras") in view of U.S. Patent Application No. 2005/0268112 to Wang *et al*. ("Wang").

Applicants responded to the non-final Office Action by amending the independent claims. Specifically, the independent claim 1 was amended to recite, in part "computer**, the method** comprising: **receiving, from a user**, establishing", and independent claim 12 was amended to recite, in part "a computer**,** including **the system comprising**:...**to detected activity activity on the computer that is indicative of pestware**~~a suspicion of pestware on the compuer~~...at least one log on **a file storage device of** the computer". Ex. 1002, pp. 193-95(underlines showing the amended language). In associated remarks, Applicants argued that claim 1

uses a user-supplied "time of interest" to guide an automated (computer-implemented) process for researching and identifying the source, and the cited references do not disclose that claim 1 feature. Ex. 1002, pp. 198-199. Applicants further that the references do not recite the claim 12 feature of "a timestamp module configured to generate a time of interest in response to detected activity on the activity on the computer that is indicative of pestware." Ex. 1002, p. 199.

A final Office Action was submitted, issued 2/22/10, that rejected claims 1-6, 8, 10-16, and 19-23. Ex. 1002, p. 162. The final Office Action rejected claims 1-6, 8, 10-16, and 19-23 under 35 U.S.C. § 103(a) as unpatentable over Porras, Wang, and further in view of U.S. Patent Application No. 2004/0225877 to Huang.

Applicants responded to the final Office Action by submitting a Request for Continued Examination and amending independent claim 1 to recite, in part "**externally networked** sources that the computer received files...**an externally networked** source that is suspected of originating pestware", and independent claim 12 to recite, in part "**externally networked** source of potential pestware activity on the computer...**externally networked** source of potential pestware activity". Ex. 1002, pp.147-49. Applicants contended that the combination of references do not teach the above added limitations to claims 1 and 12. Ex. 1002, pp. 153-54.

In the non-final Office Action, issued 9/10/10, claims 1-6, 8, 10-16, and 19-23 were rejected. Ex. 1002, p. 123. The non-final Office Action rejected claims 1-6, 8, 10-16, and 19-23 under 35 U.S.C. § 103(a) as unpatentable over Porras and U.S. Patent Application No. 2007/0168694 to Maddaloni *et al*. ("Maddaloni").

Applicants responded to the non-final Office Action by not amending any of the claims and arguing that the Maddaloni reference is disqualified as prior art under 35 U.S.C. § 103(c)(1). Ex. 1002, p. 115.

In the non-final Office Action, issued 3/28/11, claims 1-6, 8, 10-16, and 19-23 were rejected. Ex. 1002, p. 87. The non-final Office Action rejected claims 1-6, 8, 10-16, and 19-23 under 35 U.S.C. § 103(a) as unpatentable over Porras and U.S. Patent Application No. 2007/0094725 to Borders. Ex. 1002, p. 89.

Applicants responded to the non-final Office Action by amending claim 1 to recite, in part "receiving, from a user **via an interface of the computer**...accessing**, using a hardware processor of the computer,**...**wherein the recorded history of externally networked sources is stored on a file storage device**", and amending claim 12 to recite, in part " **a hardware processor; a file storage device coupled to the hardware processor;**" a timestamp, research portion, and reporting portion "**to be executed by the hardware processor**". Ex. 1002, 65-67.

Allowance of the ’244 patent followed. The Notice of Allowability, issued 1/23/12, indicated that an Examiner Interview occurred on 12/20/11 and Applicants agreed, via Examiner Amendment, to amend independent claims 1 and 12 to recite the limitations of claims 5, 19, 21 and add the limitations “issuing a timestamp after receiving the time of interest to initiate the pestware research”. Ex. 1002, p. 36. Claims 1-4, 6, 8, 10-16, 20, 22, and 23 were deemed allowed.

D. Level of Ordinary Skill in the Art

As established by the Declaration of Dr. Seth Nielson dated September 7, 2023 (*See* Ex. 1003, ¶XX), a person having ordinary skill in the art (PHOSITA) would have a B.S. degree in Computer Science, computer engineering, or an equivalent, and two years of professional experience relating to network communications. Lack of professional experience can be remedied by additional education, and vice versa. Ex.1003, ¶XX.)

E. Claim Construction

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

In parallel litigation, Webroot argued claim terms in asserted patents should be given their plain and ordinary meanings. Likewise, the claim construction order in this parallel litigation by the Western District of Texas court construed contested

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

V. Grounds of Rejection

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

A. Ground 1: Claims 1-16 are unpatentable under 35 U.S.C. § 103(a) as

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

obvious in view of Li 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 '244 patent and a more than adequate written rationale is provided to support the combination of Halperin and Inoue under *KSR.* 550 U.S. at 418.

B. Ground 1: Claims 1-16 are unpatentable under 35 U.S.C. § 103(a) as obvious in view of Li 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 '244 patent and a more than adequate written rationale is provided to support the combination of Li and Piccard under *KSR.* 550 U.S. at 418.

A PHOSITA would have been motivated to combine the teachings of Li and Piccard as both prior art documents are directed to methods of monitoring and detecting network intrusions and malware. EX1003, ¶135.

Li is directed toward methods for correlating different types of logs in order to improve intrusion detection. Li discloses "a unified logging architecture that can effectively capture correlations among entries in different types of logs … to take advantage of the naturally existing correlations among activities in different types of logs, such as network logs and system call logs." EX1008, p.1; EX1003, ¶¶126-127,135-138. Among the activity logs address in Li are a "kernel API logger [that] should record system calls, the parameters of those calls, and the time at which they are made." EX1008, p.5. In describing intrusion detection, Li uses the example of the Yaha virus as a reason to monitor activity logs to recognize increase abnormal behavior in a system infected by that virus. EX1008, p.4. Li shows that by correlating different types of logs, intrusion detection accuracy with reduced false positives can be achieved. EX1008, p.10; EX1003, ¶¶128-133,135-139.

Piccard, in the same field of endeavor, discloses methods for detecting malware, particularly teaching steps to take after identification of malware in order to identify the offending files downloaded from an external source. EX1003, ¶¶122-123,140-142; 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]. Piccard also then reports the findings of its malware identification to a remotely located computer so

as to flag the offending website or source as malicious. EX1003, ¶¶124-125,143-145; EX1007, ¶[0023]. Thus, A PHOSITA would have looked to modify Li with Piccard in order to prevent future attacks and identify common sources of malware. EX1003, ¶144.

Further, a PHOSITA would have had an expectation of success in combining the teachings of Li and Piccard since both teach data logs as the foundations for their analysis; and a PHOSITA would have understood how to combine the file-based logs of Piccard into the activity database of Li (e.g., through the file I/O monitor of Li). EX1003, ¶¶137,145.

1. Claim 1

a. A method for identifying an origin of suspected pestware activity on a computer, the method comprising:

Li teaches a system that "[a]t an intrusion,[] can be used to automatically identify the source and the execution path of the intrusion." EX1008, p.2; EX1003, ¶149-150. Likewise, Piccard teaches a method for identifying the source of malware by examining web traffic history, stating "[e]mbodiments of the invention include systems of managing malware. In one embodiment, a system includes a malware detection module configured to analyze a file of a protected computer to determine that the file is associated with malware." EX1007, ¶[0005]; EX1003, ¶¶152-153.

Therefore, both Li and Piccard render the preamble obvious to a PHOSITA.

b. monitoring, with a kernel-mode driver, activity on the computer;

Li teaches the use of "activity logging" to aggregate information from various sources on the system to better trace intrusions. EX1008, p.2; EX1003, ¶157. Li discloses multiple types of loggers that observe various aspects of system activity under a unified architecture, including kernel APIs, network activity, file system events, user behavior, system events, and application events. EX1008, p.5; EX1003, ¶158. Regarding the kernel API logger, Li describes the implementation as a "System Call Log – Generated by APISpy32, contains a list of system calls executed by all running processes on the system. We extract the system call, process ID, and time of execution." EX1003, ¶159; EX1005, p.9.

Therefore, Li renders limitation 1[b] obvious to a PHOSITA. EX1003, ¶162.

c. generating an activity log on a file storage device of the computer from the kernel-mode driver;

As described regarding claim limitation 1[b], Li teaches a system call log that "contains a list of system calls executed by all running processes on the system' and "extract[s] the system call, process ID, and time of execution." EX1003, ¶159; EX1005, p.9. Further, Li teaches using "several different loggers to capture data from multiple vantage points." EX1003, ¶¶165-167; EX1008, p.5,8. At least one of the loggers in Li is specifically described as being generated from kernel-level monitoring (which a PHOSITA would have known is from a kernel-

mode driver). *Id*. Li describes monitoring element as a "Kernel API Logger: A kernel API logger should record system calls, the parameters of those calls, and the time at which they are made," which corresponds to "c. generating an activity log on a file storage device of the computer from the kernel-mode driver". *Id*.

Therefore, Li renders limitation 1[c] obvious to a PHOSITA. EX1003, ¶170.

d. receiving, from a user via an interface of the computer, a time of interest relating to a suspicion of pestware on the computer, wherein the time of interest includes a time interval;

Li discloses a user interface that is used to query the database and to generate correlations of the aggregated activity. EX1003, ¶173. Li explains that a user interface is a core component of an Intrusion Detection System (IDS) and "enables an administrator to view output from the system and to control the behavior of the IDS." EX1003, ¶173; EX1008, p.3. This user interface allows the administrator to view specific time windows of activity (e.g., yesterday at midnight) (corresponding to "receiving, from a user via an interface of the computer, a time of interest relating to a suspicion of pestware on the computer"). EX1003, ¶174; EX1008, p.7. In general, Li describes a system that enables easy retrieval of time windows of system activity and related activity that has been correlated to activity in the selected window (corresponding to "the time of interest includes a time interval"). EX1003, ¶175-177; EX1008, p.7.

Therefore, Li renders limitation 1[d] obvious to a PHOSITA. EX1003, ¶178.

e. issuing a timestamp after receiving the time of interest;

Li discloses that all system call event records in the aggregated log file have timestamps associated with them. EX1003, ¶181; EX1008, p.6. Li also describes an interface where a time window of interest results in a SQL query with a timestamp. EX1003, ¶182; EX1008, p.7. A POSITA would have understood that all time-related SQL queries related to data with timestamps could include timestamps in the query. EX1003, ¶183. That is, a POSITA would have known that queries for data with a particular timestamp could include a timestamp in the query issued to the data base. EX1003, ¶¶183-184.

Therefore, Li renders limitation 1[e] obvious to a PHOSITA. EX1003, ¶185.

f. identifying, based upon the time of interest, indicia of pestware, wherein the identifying is initiated by the issuing the timestamp; and

Li discloses monitoring system behaviour to identify abnormal behavior that corresponds to actions of a virus (e.g., Yaha virus). EX1003, ¶189. Based on one suspicious event (e.g., searching contact lists), the system of Li will further query associated information to identify the intrusion (corresponding to "identifying, based upon the time of interest, indicia of pestware"). EX1008, pp.4,10; EX1003, ¶¶188-189. As discussed with respect to limitation 1[e], a PHOSITA would have understood that searching within a time period would include issuing timestamps to the database, or, at the very least, it would have been obvious. Thus, the

searching and identifying of the additional indications of viruses is initiated by issuing the timestamp. EX1003, ¶¶189-190.

Therefore, Li renders limitation 1[f] obvious to a PHOSITA. EX1003, ¶191.

g. accessing, using a hardware processor of the computer, at least a portion of a recorded history of externally networked sources that the computer received files from so as to identify, based at least in part upon the identified indicia of pestware, a reference to an identity of an externally networked source that is suspected of originating pestware;

Li discloses collecting data from various networking-related log files including a "Network Logger," the "WinDump Log," and the "TDIMonitor Log" in order to aggregate the logs under a unified architecture. EX1008, pp.6,10,13; EX1003, ¶¶194-195. Further, as explained regarding limitation 1[d], the system of Li accesses a subset of logged events including network events based on a selected time window (corresponding to "accessing, using a hardware processor of the computer, at least a portion of a recorded history of externally networked sources"). *Id*. Moreover, Li discloses using this network information in identifying pestware, stating "we examine the network traffic corresponding to the same time period," which corresponds to "based at least in part upon the identified indicia of pestware, a reference to an identity of an externally networked source". EX1008, p.4; EX1003, ¶195.

Further, Piccard teaches using computer to analyze a download history log (corresponding to "accessing, using a hardware processor of the computer, at least a portion of a recorded history of externally networked sources that the computer received files from") to identify the external source (e.g., URL) of a file suspected of being malware. EX1007, ¶[0005]; EX1003, ¶196. Piccard discloses that its "Web site identification module" is invoked after a determination of malware by the "malware detection module". EX1007, ¶[0015]; EX1003, ¶197. Piccard indicates that the "Web site identification module" then accesses the history log to determine the external source. *Id*.

A PHOSITA would have found it obvious to have the "malware detection module" either be or be combined with Li's IDS as described in limitation 1[f]. EX1003, ¶197. A PHOSITA would have understood a component that identifies malware to be a "malware detection module." EX1003, ¶197. Thus, it would have been obvious to have Li's IDS trigger Piccard's "Web site identification module," which action, a PHOSITA would understand to correspond to "so as to identify, based at least in part upon the identified indicia of pestware, a reference to an identity of an externally networked source that is suspected of originating pestware." EX1003, ¶¶197-201.

Therefore, Li in view of Piccard renders limitation 1[g] obvious to a PHOSITA. EX1003, ¶203.

h. wherein the recorded history of externally networked sources is stored on the file storage device.

Li discloses examining data in networking-related log files as discussed with respect to limitation 1[g] (e.g., networking log, WinDump log, and TDIMonitor log). EX1008, pp.4,10; EX1003, ¶¶206-208. A PHOSITA would have understood the logs of the systems of Li and Piccard to generally be stored on the local computer. EX1003, ¶206. Even if the networking logs were not stored locally, all logs are aggregated into the database and the aggregated log is stored locally (corresponding to "the recorded history of externally networked sources is stored on the file storage device"). EX1003, ¶207.

Therefore, Li in view of Piccard renders limitation 1[h] obvious to a PHOSITA. EX1003, ¶¶211-213.

Therefore, a PHOSITA would have found claim 1 to be obvious based on Li in view of Piccard. Accordingly, claim 1 should be found invalid under 35 U.S.C. § 103 based on Li and Piccard.

2. Claim 2

a. The method of claim 1, wherein the identifying includes: accessing at least one log of historical events on the computer;

As described regarding limitation 1[f], Li teaches examining historical event data from logs (e.g., system call activity and network activity). EX1008, p.4;

EX1003, ¶216. Further, Li teaches that activity from the various log sources are aggregated in an "activity database" to aid in querying for related information, where the queries can be time based (e.g., yesterday at midnight). EX1008, p.6; EX1003, ¶217.

Therefore, Li renders limitation 2[a] obvious to a PHOSITA. EX1003, ¶¶215,219.

b. locating at least one event in the at least one log that corresponds to the time of interest; and

As described regarding claim limitations 1[d] and 1[f], Li discloses locating events that correspond to the time of interest by identifying events that are within a time interval of the time of interest. EX1008, pp.4,7; EX1003, ¶222. Li discloses that the SQL queries can specify a time of interest in the user interface (e.g., time windows around a specific event as discussed below). *Id*. For example, Li discloses identifying events in the network traffic logs that corresponds to the time of interest (e.g., yesterday at midnight). *Id*.

Therefore, Li renders limitation 2[b] obvious to a PHOSITA. EX1003, ¶¶221,223.

c. determining that the at least one event is associated with the indicia of pestware.

As discussed with respect to limitation 2[b], Li discloses examining network traffic events corresponding to a specific time period. EX1008, p.4; EX1003, 226-

227. Li also discloses determining that these traffic events are associated with indicia of pestware by identifying them as having abnormal increases in the network traffic, confirming that an intrusion of a virus (pestware) has occurred. *Id*.

Therefore, Li renders limitation 2[b] obvious to a PHOSITA. EX1003, ¶¶225,227.

As shown, the Li-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 Li and Piccard.

3. Claim 3

The method of claim 2, wherein the determining that the at least one event is associated with the indicia of pestware includes following references in the at least one log to a suspected pestware object.

Li discloses identifying a suspected malware file and/or process, which corresponds to "a suspected pestware object", based on data within the collected log files. EX1003, ¶231. For example, Li discloses identifying all program names that belong to a given parent (program) as part of a pre-defined query, where the parent-child relationship corresponds to "following references in the at least one log file". EX1008, p.11,Table-1; EX1003, ¶231. Further, Li also discloses looking up the process name (which is either identical to or related to the file name. EX1003, ¶¶232-233; EX1008, p.4. The system is explicitly designed to enable the

tracing of intrusions to specific processes. Li explains, the system "…also supports queries from a monitor to find out correlated activities watched by other monitors, or to trace to the specific processes or users that directly or indirectly cause the occurring intrusion." *Id*.

Therefore, Li renders claim 3 obvious to a PHOSITA. EX1003, ¶234.

As shown, the Li-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 Li and Piccard.

4. Claim 4

> **The method of claim 3, wherein following the references includes following at least one reference in the activity log from the event to a suspected pestware process.**

Li discloses identifying a suspected malware file and/or process, which corresponds to "a suspected pestware object", based on data within the collected log files. EX1003, ¶237. For example, Li discloses identifying all program names that belong to a given parent (program) as part of a pre-defined query, where the parent-child relationship corresponds to "following the references includes following at least one reference in the activity log". EX1008, p.11,Table-1; EX1003, ¶237. Further, Li teaches tracing actions to actions in the activity log, including tracing intrusions to specific processes. EX1003, ¶¶238-239. Li explains, the system "…also supports queries from a monitor to find out correlated

activities watched by other monitors, or to trace to the specific processes or users that directly or indirectly cause the occurring intrusion." *Id*.

Further, Piccard teaches analyzing the file identified by a malware detection device including whether or not the file acts suspiciously. EX1003, ¶240; EX1007, ¶[0020]. A POSITA would have understood that only a file that is executing (i.e., is a process) is capable of suspicious activities such as modification to the registry file of an operating system. EX1003, ¶241. A PHOSITA would recognize that Piccard in combination with Li describes log data that identifies the file which is also combined with the activities of the associated process for the file. *Id*.

Therefore, Li in view of Piccard renders claim 4 obvious to a PHOSITA. EX1003, ¶243.

As shown, the Li-Piccard combination discloses all elements recited in claims 1, 2 and 3 from which claim 4 depends. Accordingly, claim 4 should be found invalid under 35 U.S.C. § 103 based on Li and Piccard.

5. Claim 5

The method of claim 2, wherein the at least one log includes 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 explained regarding claim limitation 1[c], the generated component logs and the generated aggregated log of Li are activity logs. EX1008, p.9; EX1003, ¶246. Likewise, as explained regarding claim limitation 1[c], these logs are event logs. EX1003, ¶247. Piccard also teaches browser history logs. EX1007, ¶[0013].

Therefore, both Li and Piccard render claim 5 obvious to a PHOSITA. EX1003, ¶248.

As shown, the Li-Piccard combination discloses all elements recited in claims 1 and 2 from which claim 5 depends. Accordingly, claim 5 should be found invalid under 35 U.S.C. § 103 based on Li and Piccard.

6. Claim 6

The method of claim 1, wherein the user input is in response to an alert provided to the user regarding a detected suspicious activity on the computer.

Li discloses that abnormal behavior can generate alerts. EX1003, ¶251. For example, "if the file I/O monitor detects many file accesses from an ordinary user [during nighttime hours], it can generate a warning that an intrusion is likely taking place." EX1008, p,6; EX1003, ¶251. Li discloses that a system with a user

interface for inputting questions related to an investigation. EX1003, ¶253; EX1008, p.3. The purpose of the interface is to make it easier for an administrator to query the system for answers to questions about behavior including within specific time windows. EX1003, ¶¶254-255; EX1008, p.7.

Piccard also discloses an alert mechanism when malware is suspected. EX1007, ¶¶[0023]-[0024]; EX1003, ¶251.

Therefore, Li renders claim 6 obvious to a PHOSITA. EX1003, ¶257.

As shown, the Li-Piccard combination discloses all elements recited in claim 1 from which claim 6 depends. Accordingly, claim 6 should be found invalid under 35 U.S.C. § 103 based on Li and Piccard.

7. Claim 7

The method of claim 1, including: reporting the identity of the externally networked source to an externally networked pestware research entity so as to enable the pestware research entity to research whether the externally networked source is a source of pestware.

As described regarding claim limitation 1[h], Piccard discloses identifying the identity of the externally networked source. EX1003, ¶260; EX1007, ¶[0023]. Piccard also discloses reporting this information to a remotely-located computer. *Id*. A POSITA would have understood that a "remotely-located computer" that "analyze[s]… to determine whether … the Web site is, in fact, a malware

distribution site" is an externally networked pestware research entity. EX1003, ¶261. This "remotely-located computer" serves the purpose of analyzing the information to determine whether the website is indeed a source of malware and subsequently reporting its findings. *Id.*

Therefore, Piccard renders claim 7 obvious to a PHOSITA. EX1003, ¶263.

As shown, the Li-Piccard combination discloses all elements recited in claim 1 from which claim 7 depends. Accordingly, claim 7 should be found invalid under 35 U.S.C. § 103 based on Li and Piccard.

8. Claim 8

a. The method of claim 1, wherein the externally networked source is identified by an identifier selected from the group consisting of an I.P. address and a URL.

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 externally networked source is identified by an identifier"). EX1007, ¶[0015]; EX1003, ¶266. Further, Piccard discloses that the recorded web address of the identified source website can be a web URL or IP address (corresponding to "an identifier selected from the group consisting of an I.P. address and a URL"). EX1007, ¶[0013],[0021]; EX1003, ¶267.

Therefore, Piccard renders claim 8 obvious to a PHOSITA. EX1003, ¶268.

As shown, the Li-Piccard combination discloses all elements recited in claim 1 from which claim 8 depends. Accordingly, claim 8 should be found invalid under 35 U.S.C. § 103 based on Li and Piccard.

9. Claim 9

a. A system for identifying a source of suspected pestware on a computer, the system comprising:

Li describes a system for dealing with intrusions, stating "This paper proposes a unified logging architecture, called UCLog, that effectively explores activity correlations for intrusion detection." EX1005, p.2; EX1003, ¶¶271-274. Likewise, Piccard teaches a system for identifying the source of malware by examining web traffic history, stating "Embodiments of the invention include systems of managing malware. In one embodiment, a system includes a malware detection module configured to analyze a file of a protected computer to determine that the file is associated with malware." EX1007, ¶[0005]; EX1003, ¶275.

Therefore, Li and Piccard both render the preamble obvious to a PHOSITA. EX1003, ¶277.

b. a hardware processor;

Li discloses an implementation on a computer system, stating "We have implemented the UCLog architecture on a real system running Microsoft Outlook Express on Windows 2000." EX1008, p.2; EX1003, ¶280. A PHOSITA would

have understood a computer system that runs Windows 2000 to have a hardware processor. Id. Likewise, Piccard teaches this limitation. EX1003, ¶281; EX1007, ¶[0012].

Therefore, Li and Piccard both render limitation 9[b] obvious to a PHOSITA. EX1003, ¶282.

c. a file storage device coupled to the hardware processor;

Li discloses that the logged data is stored in an activity database that consists of a set of tables. EX1003, ¶¶285-287; EX1008, pp.6,8,Figure-2. "The activity database consists of a set of tables, each corresponding to the filtered log entries from a monitor." *Id*. A POSITA would have understood that the activity database, including its tables, are stored on a file storage device connected to the hardware processor. EX1003, ¶¶287-288. Likewise, Piccard teaches this limitation. EX1003, ¶¶289-290; EX1007, ¶[0026].

Therefore, Li and Piccard both render limitation 9[c] obvious to a PHOSITA. EX1003, ¶291.

d. a timestamp module configured to be executed by the hardware processor, to generate a time of interest including a time interval in response to detected activity on the computer that is indicative of pestware, to issue a timestamp after generating the time of interest, and to initiate, in response to the issuance of the timestamp, identification of indicia of pestware;

The language of limitation 9[d] is almost identical to the language of limitations 1[d], 1[e], and 1[f] together. The only significant difference is that limitation 9[d] requires a timestamp "module" to perform the operations. For further details on the actions of this limitation see limitations 1[d], 1[e], and 1[f] above. EX1003, ¶294. Li also teaches a timestamp module as part of the activity database functionality. EX1003, ¶¶295-296; EX1008, pp.6,7.

Therefore, Li renders limitation 9[d] obvious to a PHOSITA. EX1003, ¶298.

e. a research portion configured to be executed by the hardware processor and to access at least one log on a file storage device of the computer to relate the time of interest to at least one externally networked source of potential pestware activity on the computer;

The language of limitation 9[e] is similar to the language of Claim 2. The only significant difference is "a research portion" that performs the operations. A POSITA would have understood the IDS components, as disclosed by Li, that access a log file combined with the Web site identification module that identifies the external networked source to be a "research portion. EX1003, ¶¶301-302.

Therefore, Li renders limitation 9[e] obvious to a PHOSITA. EX1003, ¶304.

f. a kernel-mode driver configured to monitor activity on the computer and to generate an activity log that is included within the at least one log; and

The language of limitation 9[f] is similar to the language of limitation 1[b]. For further details see the arguments of limitation 1[b]. Therefore, Li renders limitation 9[f] obvious to a PHOSITA. EX1003, ¶308.

g. a reporting portion configured to be executed by the hardware processor and to generate a report that identifies the at least one externally networked source of potential pestware activity.

The language of limitation 9[g] is similar to limitation 1[g]. The only significant change is that the operations must be performed by "a reporting portion" and that the reporting portion must "generate a report." Piccard discloses structure that generates reports. EX1003, ¶¶313-314. Therefore, Li renders limitation 9[g] obvious to a PHOSITA. EX1003, ¶315.

Therefore, a PHOSITA would have found claim 9 to be obvious based on Li in view of Piccard. Accordingly, claim 9 should be found invalid under 35 U.S.C. § 103 based on Li and Piccard.

10. Claim 10

> **The system of claim 9, wherein the at least one log includes information that relates the time of interest to an event, and wherein the at least one log includes information that relates the event to a suspected pestware object, and wherein the at least one log includes information that relates the suspected pestware object to the at least one externally networked source of potential pestware activity.**

The language of Claim 10 is similar to language found in Claims 2, 4, and 8. Accordingly, the arguments for those claims apply here as well. EX1003, ¶319.

As shown, the Li-Piccard combination discloses all elements recited in claims 9 from which claim 10 depends. Accordingly, claim 10 should be found invalid under 35 U.S.C. § 103 based on Li and Piccard.

11. Claim 11

> **The system of claim 10, including: a heuristics module configured to be executed by the hardware processor and to evaluate whether the event is a suspected pestware-related event before the research portion accesses information in the at least one log that relates the event to the suspected pestware object.**

Li discloses using RIPPER, which it describes as a "data mining" technique, to train on recognizing good and bad sequences of system calls. The rules generated from this component are used to identify abnormal system calls that indicate a possible intrusion. EX1008, pp.3-4; EX1003, ¶¶323-324. As indicated by Li, the heuristics of the RIPPER system suggest a possible intrusion. *Id*. Li explains in detail that the RIPPER system is used as part of the rule generation system. *Id*. While one part of the system uses rules for known attacks, the RIPPER

component is part of behavioral/heuristic detection that can identify previously unseen intrusions. EX1008, p.7; EX1003, ¶¶324-325. This leads to further investigation using the research module, as discussed in limitation 9[e] in order to further ascertain whether an intrusion has, in fact, taken place. *Id.*

A POSITA would have understood that identifying abnormal system call sequences against training data (or other statistical models) is an example of a "heuristic" that makes an estimate or guess as to the classification of a test input. EX1003, ¶328. A "heuristics-based detection engine" may look for behaviors commonly exhibited by malware in order to identify suspected malware, even when other detection mechanisms would not have discovered it (e.g., a never-before-seen virus that does not yet have a signature in the database of an antivirus scanner). EX1003, ¶328 (citing EX1015, pp.11-12).

As shown, the Li-Piccard combination discloses all elements recited in claims 9 and 10 from which claim 11 depends. Accordingly, claim 11 should be found invalid under 35 U.S.C. § 103 based on Li and Piccard.

12. Claim 12

> **The system of claim 11, wherein the heuristics module determines that the at least one event is suspected to be pestware-related by analyzing other events in connection with the event, wherein the other events are also related to the time of interest.**

As explained with respect to Claim 11, Li discloses correlating multiple activity log events together, such as system calls and network traffic. Li explains that correlating data from multiple event logs is a key design of the system: "[c]orrelating activities from all involved components and then analyzing them together would give the IDS a better picture of the system, increasing the detection accuracy and reducing the false positives." EX1008, pp.1-2; EX1003, ¶332. The architecture disclosed by Li performs correlation: "[t]his paper proposes a unified logging architecture, called UCLog, that effectively explores activity correlations for intrusion detection." EX1008, p.2; EX1003, ¶332. Li states this again, staying "UCLog effectively exploits activity correlations between different components to improve the accuracy of intrusion detection and to reduce the number of false positives." *Id*. Li also discloses that practical tests were conducted the proved the effectiveness: "we have studied how correlating activities from the system call sequence, network activity, and file I/O operations can improve the intrusion detection accuracy." *Id*.

Moreover, Li explains in detail that the RIPPER system is used as part of the rule generation system. While one part of the system uses rules for known attacks,

the RIPPER component is part of behavioral/heuristic detection that can identify previously unseen intrusions. EX1003, ¶¶334-336.

As shown, the Li-Piccard combination discloses all elements recited in claims 9, 10, and 11 from which claim 12 depends. Accordingly, claim 12 should be found invalid under 35 U.S.C. § 103 based on Li and Piccard.

13. Claim 13

> **The system of claim 9, wherein the at least one log includes 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.**

This claim is virtually identical to Claim 5. Please see the claim 5 analysis. EX1003, ¶339. As shown, the Li-Piccard combination discloses all elements recited in claim 9 from which claim 13 depends. Accordingly, claim 13 should be found invalid under 35 U.S.C. § 103 based on Li and Piccard.

14.Claim 14

> **The system of claim 9, wherein the timestamp module is further configured to generate the time of interest as a point in time.**

As explained regarding limitation 9[d], Li discloses a time of interest which includes a time interval. However, Li also discloses a "point in time" as well. Specifically, Li discloses identifying a "point in time". EX1003, ¶342; EX1008,

p.7. As shown, the Li-Piccard combination discloses all elements recited in claim 9 from which claim 14 depends. Accordingly, claim 14 should be found invalid under 35 U.S.C. § 103 based on Li and Piccard.

15. Claim 15

> **The system of claim 9, wherein the at least one externally networked source of potential pestware activity is identified by an identifier selected from the group consisting of an I.P. address and a URL.**

This claim is virtually identical to Claim 8. Please see the claim 8 analysis. EX1003, ¶345. As shown, the Li-Piccard combination discloses all elements recited in claim 9 from which claim 15 depends. Accordingly, claim 15 should be found invalid under 35 U.S.C. § 103 based on Li and Piccard.

16. Claim 16

> **The system of claim 9, wherein the at least one log includes 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.**

This claim is exactly identical to Claim 13. Please see the claim 13 analysis. EX1003, ¶347. As shown, the Li-Piccard combination discloses all elements recited in claim 9 from which claim 16 depends. Accordingly, claim 16 should be found invalid under 35 U.S.C. § 103 based on Li and Piccard.

C. Ground 2: Claims 1-16 are unpatentable under 35 U.S.C. § 103 as obvious in view of Chen and Piccard.

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

A PHOSITA would have been motivated to combine the teachings of Li and Piccard as both prior art documents are directed to methods of monitoring and detecting network intrusions and malware. EX1003, ¶349.

Chen discloses obtaining activity logs from several sources in a computing system and consolidating the logs into a database for use in forensic analysis of intrusion events, such as malware. EX. 1006, p.1. Chen describes log processing techniques utilized, and the nature of the database and query engine that had been developed. *Id*. Chen discloses finding that a "cross-correlation of event information emanating from heterogeneous logs potentially provides a powerful basis for the forensic identification of scenarios of interest." *Id*. at p.9. Chen discloses a user interface for querying the stored activity information that allows users to specify timestamps and observe correlations of activities among the data. EX1003, ¶120. Thus, Chen focuses on tools that will facilitate the investigation of computer and network events and activities that may indicate an intrusion or unusual behavior by analyzing activity logs drawn from several sources.

Piccard, in the same field of endeavor, discloses methods for detecting malware, particularly teaching steps to take after identification of malware in order to identify the offending files downloaded from an external source. EX1003, ¶¶122-123,140-142, 352; 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]; EX1003, ¶353. Once a suspicious file is identified, a "Web site identification module" is responsible for determining the source of the file, such as accessing the browser history log that contains information about the source of downloaded files. EX1003, ¶123. Piccard also reports the findings of its malware identification to a remotely located computer so as to flag the offending website or source as malicious. EX1003, ¶¶124-125,143-145; EX1007, [0023].

A POSITA would have recognized that Chen's teachings of forensically identifying malicious software, including software downloaded via browser, align with Piccard's disclosures of its "malware detection module". 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 POSITA would have expected a high degree of success implementing Chen's techniques as part of Piccard's malware detection module. EX1003, ¶354.

Also, because Chen anticipates the ongoing expansion of multiple types of activity information as it becomes available (EX1006, pp. 2), a POSITA would have been motivated to include, as a further source of activity information, Piccard's disclosures of using the web history log to determine the source of the suspected malware. Chen already discloses using browser logs and browser caches so, to the extent these do not include a web history log, it would have been obvious to add it. *Id*. at ¶355.

Chen is also directed to forensic analysis. As Chen states, "The strategic purpose of the research has been to develop a means by which a consolidated repository of such event information can be constituted and then queried in order to provide an investigator with post hoc event correlation for forensics purposes (ECF)." EX1006, p. 1. Chen further teaches the need to correlate information on a network level using, for example, Apache logs. This concept is analogous in form and similar in purpose to concepts taught by Piccard's identification and reporting modules. Piccard teaches identifying the origin of pestware (e.g., a URL) and sharing that information with a research entity in order to provide better detection capabilities to nodes on the network. Furthermore, Piccard teaches a "malware detection module" with various exemplary techniques for detecting malware. A POSITA would have been motivated to use Piccard especially if Apache log files are not available. EX1003, ¶356.

A POSITA would have recognized that Chen's teachings of forensically identifying malicious software, including software downloaded via browser, align with Piccard's disclosures of its "malware detection module". 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 POSITA would have expected a high degree of success implementing Chen's techniques as part of Piccard's malware detection module. EX1003, ¶354.

17. Claim 1

a. A method for identifying an origin of suspected pestware activity on a computer, the method comprising:

Chen and Piccard both disclose the preamble of Claim 1. Chen discloses a method of enabling and improving forensic analysis of computer systems and software to provide event information to support an investigator with post hoc event correlation for forensic (ECF) purposes. EX1006, p. 1; EX1003, ¶360. In a similar vein of research, Piccard discloses methods for identifying the source of malware by examining web traffic history. EX1003, ¶364. Therefore, both Chen and Piccard disclose the preamble of claim 1.

b. monitoring, with a kernel-mode driver, activity on the computer;

Chen discloses obtaining data from the "Windows 2000 Security Log", which is a log that is generated by a kernel-level component of the operating system. EX1006, p. 4-5; EX1003, ¶369. A POSITA would have understood that audit information found in the Windows 2000 Security Log is generated by the Security Reference Monitor, which is a kernel component that monitors security events. EX1003, ¶370. Therefore, a PHOSITA would have found this limitation to be disclosed by Chen. *Id*. at ¶375.

c. generating an activity log on a file storage device of the computer from the kernel-mode driver;

Chen discloses consolidating many log files produced by systems, including logs of "system event[s], audit [events], and door [events]," which a POSITA would have understood to be "activity" events, and the corresponding logs to be both event logs and activity logs. *Id*. at ¶378. A PHOSITA would understand that the Windows 2000 Security Log generated by a kernel-level component of the operating system is stored on a file storage device (corresponding to "an activity log on a file storage device of the computer from the kernel-mode driver"). *Id*. at ¶¶379,381. Further, Chen discloses generating a new composite log combined from all the log sources, as illustrated in Figure 1, which is reproduced below. *Id*. at ¶380. This figure illustrates that the composit log is saved on a "database,"

which necessarily is saved in computer memory. Therefore, a PHOSITA would have found this limitation to be disclosed by Chen. *Id*. at ¶383.

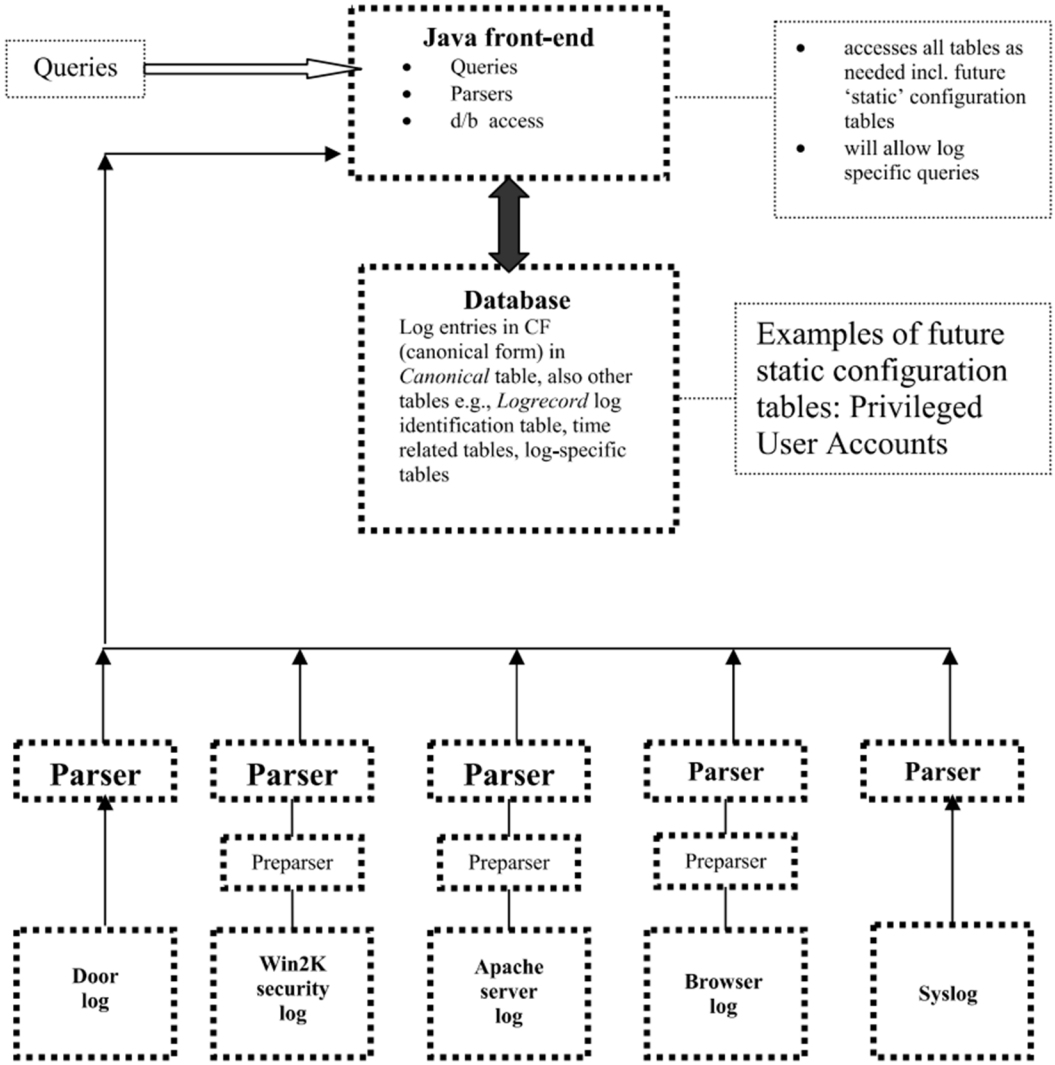

Figure 1: The ECF Architecture

EX1006, p. 3.

d. receiving, from a user via an interface of the computer, a time of interest relating to a suspicion of pestware on the computer, wherein the time of interest includes a time interval;

Chen discloses a user interface that permits an administrator to query events using SQL queries, which can specify a time of interest (e.g., time windows around a specific event). EX1006, p. 8; EX1003, ¶¶386-388. Specifically, Chen explains that time constraints (e.g., "within 10 minutes") could be expressed in a Dynamic Query interface, as well as disclosing a "Custom Query" for creating flexible SQL queries. EX1006, p. 4; EX1003, ¶¶388-370. Therefore, a PHOSITA would have found this limitation to be disclosed by Chen. *Id*. at ¶392.

e. issuing a timestamp after receiving the time of interest;

Chen discloses identifying and the beginning and ending of a ten-minute window of the designated event. Chen discloses issuing timestamps ("time values" e.g., "starttime") related to events, as well as enabling an investigator to identify a time or time window of interest that with the system using such timestamps to find all events within the time period. EX1006, pp. 4, 8; EX1003, ¶¶373-374. Therefore, a PHOSITA would have found this limitation to be disclosed by Chen. *Id*. at ¶376.

f. identifying, based upon the time of interest, indicia of pestware, wherein the identifying is initiated by the issuing the timestamp; and

As discussed re 1[e], Chen discloses issuing timestamps ("time values") so that all events within a time period identified by an investigator can be found. EX1006, pp. 4, 8; EX1003, ¶¶373-374. Chen discloses providing forensic data in order to identify pestware (example: software that elevates Windows privileges), using time values in order for the system to find all events within the time period of an "event" that the investigator is researching. *Id*. Chen provides examples of indicia of events (which would include "pestware"), including users that logged into a particular workstation within a time window, activities on that workstation during the time window, files downloaded to a particular person during the time window, and particular files downloaded during the time window, with the time window tied to time stamps (e.g., "2003-08-08 04:56:28"). EX1006, pp. 8-9. Chen also discloses that the methods could be automated. EX1006, p. 9; EX1003, ¶380. Therefore, a PHOSITA would have found this limitation to be disclosed by Chen. EX1003, ¶381.

g. accessing, using a hardware processor of the computer, at least a portion of a recorded history of externally networked sources that the computer received files from so as to identify, based at least in part upon the identified indicia of pestware, a reference to an identity of an externally networked source that is suspected of originating pestware;

As discussed with re 1[f], Chen discloses identifying indicia of pestware including specific files names. Chen also discloses using web browser logs, which would provide a portion of a recorded history of externally networked sources from which the computer received files. Id. at 384. Further, Chen discloses using browser logs (e.g., Apache files) in identifying potential malware. EX1006, p. 8; EX1003, ¶385.

Piccard also teaches using a download history log of externally networked sources to identify the external source (e.g., URL) of a file suspected of being malware. EX1007, [0005]; EX1003, ¶386. In particular, Piccard discloses that the "Web site identification module" is invoked after a determination of malware by the "malware detection module," such as Chen's ECF. EX1007, [0015]; EX1003, ¶387. Piccard discloses determining "a Web address from which the file was received" which is consistent with "identify, based at least in part upon the identified indicia of pestware, a reference to an identity of an externally networked source that is suspected of originating pestware." EX1003, ¶389.

Therefore, a PHOSITA would have found this limitation to be disclosed by Chen in view of Piccard. *Id*. at ¶376.

h. wherein the recorded history of externally networked sources is stored on the file storage device.

Chen discloses examining data in Apache log files that the ECF copies into its database, which is stored locally on the ECF's system. *Id*. at ¶393*; see also* Figure 1 of Chen reproduced above. Similarly, Piccard discloses storing a history log 116 maintained by the web browser 114 in memory (e.g., memory 112), and the web site identification module 120 accessing this history log to identify the web address of a file, which may identify a potential malware distribution site. EX1007, [0013],[0015]; EX1003, ¶395. Therefore, a PHOSITA would have found this limitation to be disclosed by Chen in view of Piccard. EX1003, ¶397.

Therefore, a PHOSITA would have found claim 1 to be obvious based on Chen in view of Piccard. Accordingly, claim 1 should be found invalid under 35 U.S.C. § 103 based on Chen and Piccard.

18. Claim 2

a. The method of claim 1, wherein the identifying includes: accessing at least one log of historical events on the computer;

As discussed regarding claim 1, Chen discloses accessing logs that store historical events information and consolidating the logs into a database that can be used for forensic analysis. *Id*. at ¶402; EX1006, p. 1. This is illustrated in Chen

Figure 1 reproduced here that shows the database for access via queries presented through a Java front-end.

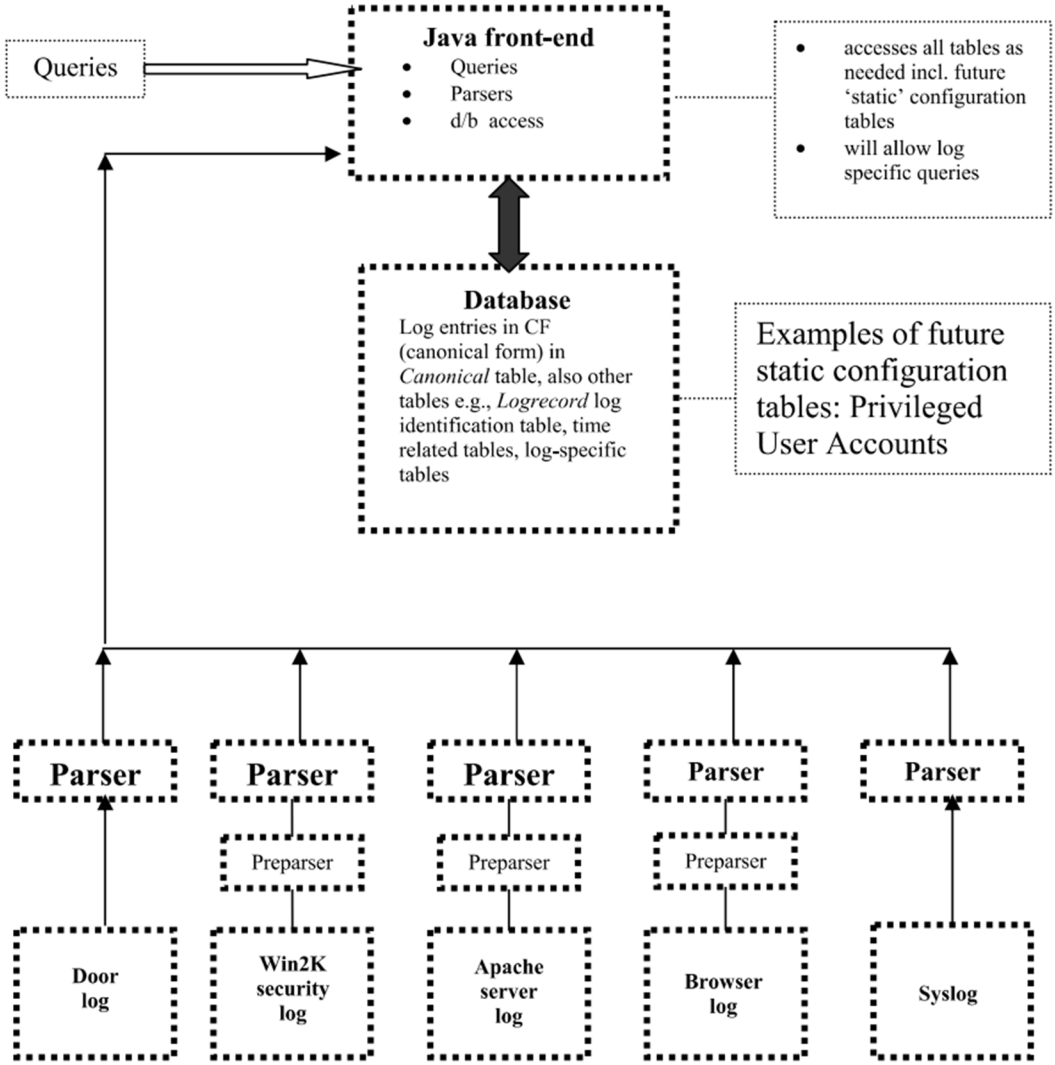

Figure 1: The ECF Architecture

Therefore, a PHOSITA would have found this limitation to be disclosed by Chen. EX1003, ¶405.

b. locating at least one event in the at least one log that corresponds to the time of interest; and

As discussed regarding 1[e]-1[g], Chen discloses locating events that correspond to the time of interest by identifying events that are within an interval of the time of interest based on time values ("timestamps") of events in the log. *Id*. at ¶¶373-385, 408-414. Therefore, a PHOSITA would have found this limitation to be disclosed by Chen. *Id*. at ¶415.

c. determining that the at least one event is associated with the indicia of pestware.

As discussed re 1[g], Chen discloses that the events identified within the time window can be determined to be indicia of malicious software (pestware). *Id*. at ¶418. Therefore, a PHOSITA would have found this limitation to be disclosed by Chen. *Id*. at ¶419. As shown, the Chen-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 Chen and Piccard.

19. Claim 3

The method of claim 2, wherein the determining that the at least one event is associated with the indicia of pestware includes following references in the at least one log to a suspected pestware object.

Chen discloses identifying a suspected malware file, which is a pestware object, based on data within the log files. *Id*. at ¶423. In particular, Chen discloses:

> ***The files 'rawrite2.exe' and 'bd030426.bin' actually relate to the exploit in this case***. The 'rawrite2.exe' utility is a tool for copying bootable floppy disk images to a floppy disk. The image file, in this case 'bd030426.bin', contains a utility for wiping the Windows administrator password (on vulnerable Windows 2000 hosts). ***These logs give us a very strong indication of what actually happened in this case***.

EX1006, p. 9 (emphasis added).

Therefore, a PHOSITA would have found this limitation to be disclosed by Chen. EX1003, ¶424. As shown, the Chen-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 Chen and Piccard.

20. Claim 4

The method of claim 3, wherein following the references includes following at least one reference in the activity log from the event to a suspected pestware process.

As discussed re claim 3, Chen discloses identifying file objects associated with the suspected pestware, using the example of "copying bootable floppy disk images to a floppy disk." EX1006, p.9; EX1003, ¶¶ 423, 426.

Piccard teaches analyzing the file identified by a malware detection device including whether or not the file acts suspiciously. EX1003, ¶428; EX1006, [0020]. A POSITA would have understood that only a file that is executing (i.e., is a process) is capable of suspicious activities such as modification to the registry file of an operating system, and the activities of the executing process would be recording in the consolidate log file described in Chen. EX1003, ¶429.

Therefore, a PHOSITA would have found this limitation to be disclosed by Chen in view of Piccard. *Id*. at ¶431. As shown, the Chen-Piccard combination discloses all elements recited in claims 1-3 from which claim 4 depends. Accordingly, claim 4 should be found invalid under 35 U.S.C. § 103 based on Chen and Piccard.

21. Claim 5

> **The method of claim 2, wherein the at least one log includes 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 discussed re 1[c], Chen discloses activity logs, such as the Windows 2000 Security Log, as well as event logs, such as browser logs and browser cache logs. *Id*. at ¶¶434-435. Therefore, a PHOSITA would have found this limitation to be disclosed by Chen. *Id*. at ¶436. As shown, the Chen-Piccard combination discloses all elements recited in claims 1 and 2 from which claim 5 depends. Accordingly, claim 5 should be found invalid under 35 U.S.C. § 103 based on Chen and Piccard.

22. Claim 6

> **The method of claim 1, wherein the user input is in response to an alert provided to the user regarding a detected suspicious activity on the computer.**

Chen discloses the use of forensic operations in response to a suspicious event, such as an unexpected password change may be suspicious and this can trigger an investigation. *Id*. at ¶439. As Chen explains:

> In this case the investigator may have very little idea about the exact nature of the scenario above, but will most likely become suspicious upon noticing that the Administrator password has

> changed. This discovery may not occur until some time after the exploit was actually carried out.

EX1006, p. 8.

Piccard also discloses an alert mechanism when malware is suspected:

> In the illustrated embodiment, once the Web site identification module identifies the Web site, a reporting module (e.g., the reporting module 122) reports information regarding the Web site to a remotely-located computer that is connected to the protected computer. This information can identify the Web site as a potential malware distribution site, such as in terms of the domain name of the Web site. Alternatively, or in conjunction, this information can identify the file as including potential malware, Such as in terms of the name of the file or the URL of the file. It is also contemplated that this information can include a representation of the file or can identify suspicious activities related to the file.
>
> In the illustrated embodiment, the reporting module also alerts a user of the protected computer about the Web site.

EX1007, [0023]-[0024].

To the extent Chen does not disclose this limitation alone, it would have been obvious to a POSITA in view of Piccard's disclosures.

Therefore, a PHOSITA would have found this limitation to be disclosed by Chen as well as Chen in view of Piccard. EX1003, ¶436. As shown, the Chen-

Piccard combination discloses all elements recited in claim 1 from which claim 6 depends. Accordingly, claim 6 should be found invalid under 35 U.S.C. § 103 based on Chen and Piccard.

23. Claim 7

> **The method of claim 1, including: reporting the identity of the externally networked source to an externally networked pestware research entity so as to enable the pestware research entity to research whether the externally networked source is a source of pestware.**

Piccard discloses identifying the identity of the externally networked source. Piccard also discloses reporting this information to a remotely-located computer. EX1003, ¶444. Piccard explains:

> The third operation illustrated in FIG. 2 is to report that the Web site is a potential malware distribution site (block 204). In the illustrated embodiment, once the Web site identification module identifies the Web site, a reporting module (e.g., the reporting module 122) reports information regarding the Web site **to a remotely-located computer** that is connected to the protected computer. This information can identify the Web site as a potential malware distribution site, such as in terms of the domain name of the Web site… **This information as well as any additional relevant information can be analyzed at the remotely-located computer to determine whether the file**

> **does, in fact, include malware** and whether the Web site is, in fact, a malware distribution site.

EX1007, [0023] (emphasis added).

A POSITA would have understood that a "remotely-located computer" that "analyze[s]… to determine whether the file does, in fact, include malware" is the same thing as an externally networked pestware research entity. EX1003, ¶445.

Therefore, a PHOSITA would have found this limitation to be disclosed by Piccard. EX1003, ¶447. As shown, the Chen-Piccard combination discloses all elements recited in claim 1 from which claim 7 depends. Accordingly, claim 7 should be found invalid under 35 U.S.C. § 103 based on Chen and Piccard.

24. Claim 8

> **The method of claim 1, wherein the externally networked source is identified by an identifier selected from the group consisting of an I.P. address and a URL.**

Piccard discloses identifying the external network source of the potential pestware by both IP address and URL. EX1003, ¶450. Piccard explains:

> As illustrated in FIG.1, the memory 112 also stores a history log 116, which is maintained by the Web browser 114 to provide a record of browsing events. In particular, when a file is accessed and downloaded, the W**eb browser 114 records a Web address of the file in the history log 116**. A Web address typically specifies a location of a file within a Web site. For example, a **Web address can be a Uniform Resource Identifier ("URI) of**

> **a file, such as a Uniform Resource Locator ("URL) of the file.** It is also contemplated that a Web address can be defined in various other ways, such as using an Internet Protocol ("IP) address **or any other identifier of a source of a file**.

EX1007, [0013], (emphasis added).

Therefore, a PHOSITA would have found this limitation to be disclosed by Piccard. EX1003, ¶452. As shown, the Chen-Piccard combination discloses all elements recited in claim 1 from which claim 8 depends. Accordingly, claim 8 should be found invalid under 35 U.S.C. § 103 based on Chen and Piccard.

25. Claim 9

a. A system for identifying a source of suspected pestware on a computer, the system comprising:

Chen and Piccard both disclose systems consistent with the preamble of Claim 9. As discussed, Chen discloses a system of enabling and improving forensic analysis of computer systems and software. (See for example Figure 1 reproduced above.) Piccard also teaches a system for identifying the source of malware by examining web traffic history, including a detailed description of the system components and modules with reference to FIG. 1, which is reproduced below. EX1007, [0012]-[0017]. Therefore, both Chen and Piccard disclose the preamble of claim 9.

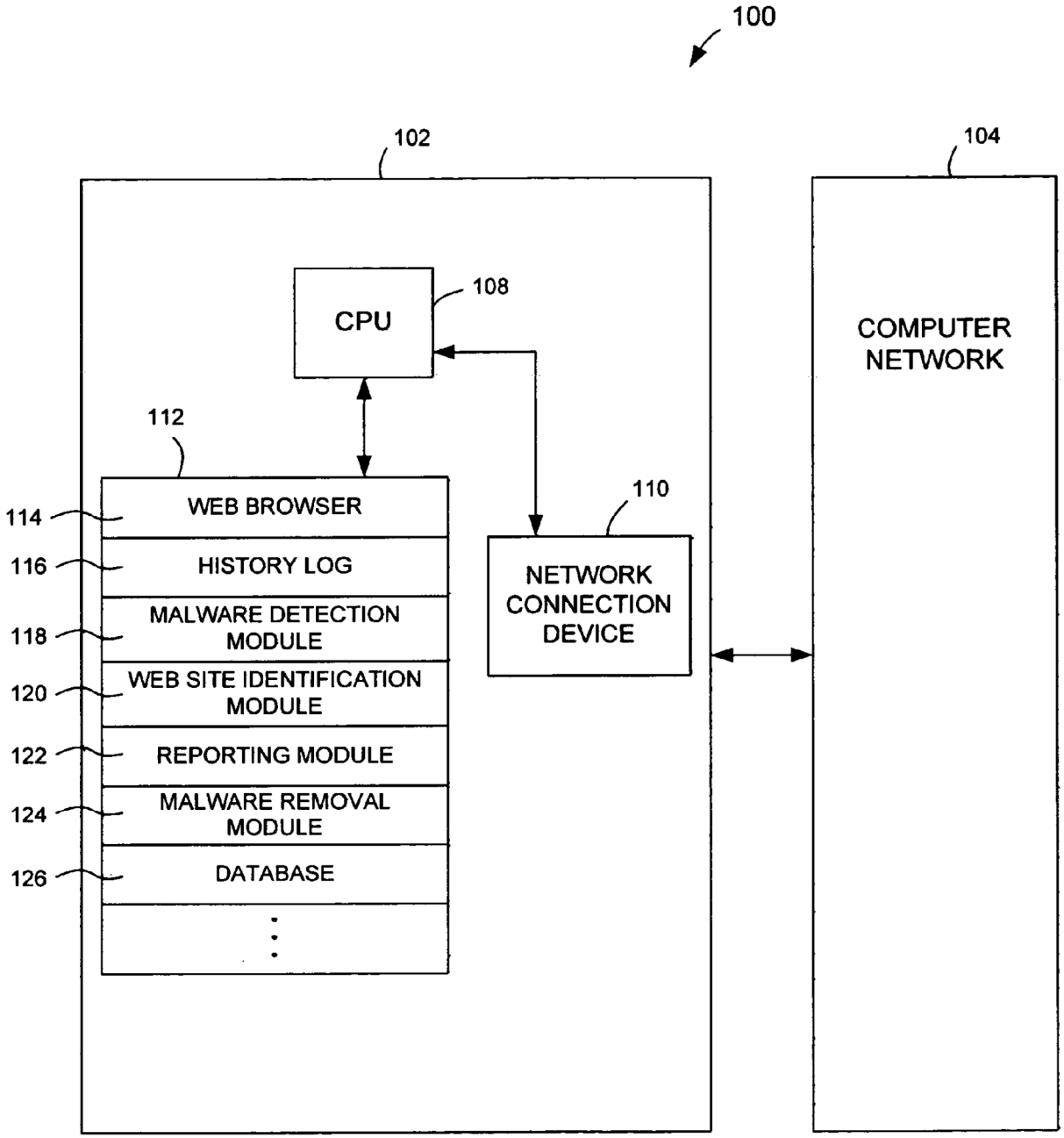

FIG. 1

EX1007, FIG. 1.

b. a hardware processor;

Chen discloses a system that makes use of Java and a Postgres database, which a POSITA would have known executes on a hardware processor. EX1003, ¶465. As discussed above re 9[a] and illustrated in FIG. 1 reproduced above, Piccard discloses a system 100 that includes a CPU 108, which is a hardware processor. *Id*. at ¶466. Therefore, a PHOSITA would have found this limitation to be disclosed by both Chen and Piccard. *Id*. at ¶467.

c. a file storage device coupled to the hardware processor;

Chen discloses a system that makes use of Java and a Postgres database, which a POSITA would have known require a file storage device, such as a hard drive. *Id*. at ¶470. As discussed above re 9[a] and illustrated in FIG. 1 reproduced above, Piccard discloses a system 100 that includes a CPU 108 connected to memory 112. *Id*. at ¶471. Therefore, a PHOSITA would have found this limitation to be disclosed by both Chen and Piccard. *Id*. at ¶472.

d. a timestamp module configured to be executed by the hardware processor, to generate a time of interest including a time interval in response to detected activity on the computer that is indicative of pestware, to issue a timestamp after generating the time of interest, and to initiate, in response to the issuance of the timestamp, identification of indicia of pestware;

The language of this limitation is similar to limitations 1[d], 1[e], and 1[f] discussed above, except that this requires a timestamp "module" to perform the operations recited in those limitations. Thus, the analysis regarding 1[d], 1[e], and 1[f] apply equally here. Further, Chen also discloses a timestamp module in that the ECF Dynamic Query module issues timestamps related to suspicious events in order for the system to find all events within the time period as describe in more detail above. *Id*. at ¶476. Therefore, a PHOSITA would have found this limitation to be disclosed by both Chen. *Id*. at ¶480.

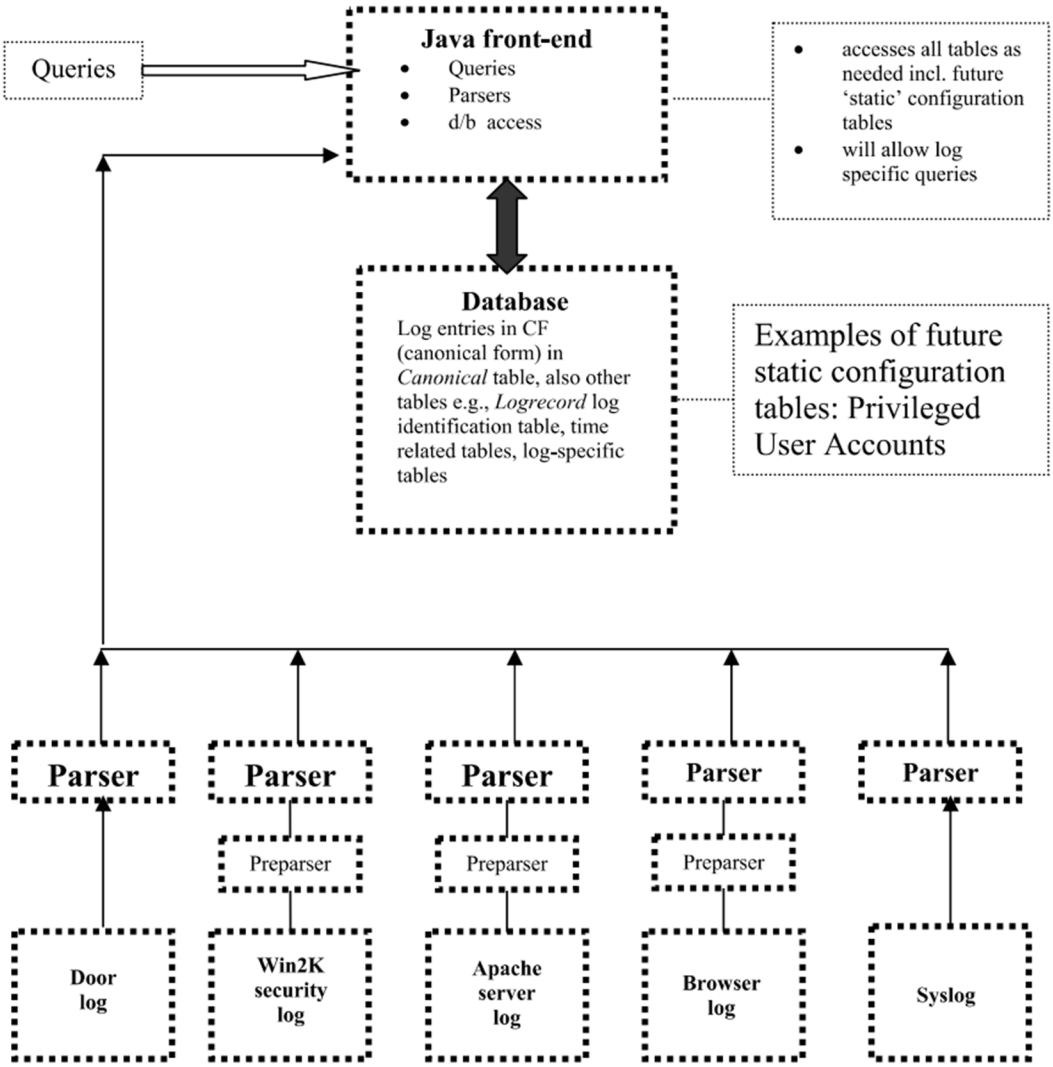

Figure 1: The ECF Architecture

e. a research portion configured to be executed by the hardware processor and to access at least one log on a file storage device of the computer to relate the time of interest to at least one externally networked source of potential pestware activity on the computer;

The language of this limitation is similar to claim 2 except reciting "a research portion" that performs the operations of claim 2. As shown re claim 2, Chen discloses accessing logs that store historical events information and

consolidating the logs into a database that can be used for forensic analysis, locating events that correspond to the time of interest by identifying events that are within an interval of the time of interest based on time values ("timestamps") of events, and determining that events identified within the time window can be indicia of malicious software (pestware). *Id*. at ¶¶402-419,483. See also Figure 1 reproduced above. Further, because Chen provides a system for performing forensic investigations into network and computer events (e.g., indicative of pestware), the components ECF components illustrated in Figure 1 show a research function in the form of the log file database and the Java front-end. A POSITA would have understood the ECF components that access a log file combined with the Web site identification module that identifies the external networked source to be a "research portion" of the system. These components are executed by the hardware processor (as they are part of the software), access the file storage device of the computer, and relate the time of interest to an externally networked source of potential pestware activity. *Id*. at ¶484. Therefore, a PHOSITA would have found this limitation to be disclosed by Chen. *Id*. at ¶487.

f. a kernel-mode driver configured to monitor activity on the computer and to generate an activity log that is included within the at least one log; and

This limitation is similar to 1[b]. As discussed re 1[b], Chen discloses obtaining data from the "Windows 2000 Security Log", which is a log that is generated by a kernel-level component of the operating system. EX1006, p. 4-5; EX1003, ¶347. A POSITA would have understood that audit information found in the Windows 2000 Security Log is generated by the Security Reference Monitor, which is a kernel component that monitors security events. EX1003, ¶348. Therefore, a PHOSITA would have found this limitation to be disclosed by Chen. *Id*. at ¶512.

g. a reporting portion configured to be executed by the hardware processor and to generate a report that identifies the at least one externally networked source of potential pestware activity.

Piccard discloses generating a report.

> The third operation illustrated in FIG. 2 is to report that the Web site is a potential malware distribution site (block 204). In the illustrated embodiment, once the Web site identification module identifies the Web site, **a reporting module (e.g., the reporting module 122) reports information regarding the Web site to a remotely-located computer that is connected to the protected computer.** This information can identify the Web site as a potential malware distribution site, such as in terms of the domain name of the Web site. Alternatively, or in conjunction,

> this information can identify the file as including potential malware, such as in terms of the name of the file or the URL of the file. It is also contemplated that this information can include a representation of the file or can identify suspicious activities related to the file. **This information as well as any additional relevant information can be analyzed at the remotely-located computer to determine whether the file does, in fact, include malware and whether the Web site is, in fact, a malware distribution site.** If the Web site is determined to be a malware distribution site, a new or updated set of malware definitions can be generated based on content within the Web site, and the new or updated set of malware definitions can be provided to the protected computer. In addition, content within the Web site can be monitored on a periodic or other basis for new or updated malware. Also, a new or updated list of malware distribution sites can be generated so as to identify the Web site, and the new or updated list of malware distribution sites can be provided to the protected computer.

EX1007, [0023] (emphasis added).

A POSITA would have understood Piccard's reporting module to be a "reporting portion" and that reporting information by the reporting portion is equivalent to "generating a report." EX1003, ¶519. Therefore, a PHOSITA would have found this limitation to be disclosed by Piccard. *Id*. at ¶520.

Therefore, a PHOSITA would have found claim 9 to be obvious based on Chen in view of Piccard. Accordingly, claim 9 should be found invalid under 35 U.S.C. § 103 based on Chen and Piccard.

26. Claim 10

> **The system of claim 9, wherein the at least one log includes information that relates the time of interest to an event, and wherein the at least one log includes information that relates the event to a suspected pestware object, and wherein the at least one log includes information that relates the suspected pestware object to the at least one externally networked source of potential pestware activity.**

The limitations recited in claim 10 are similar to language recited in dependent claims 2, 4, and 8. As describe re claim 2, Chen discloses locating events that correspond to the time of interest by identifying events that are within an interval of the time of interest based on time values ("timestamps") of events in the log, and Chen discloses that the events identified within the time window can be determined to be indicia of malicious software (pestware). *Id*. at ¶¶373-385, 408-418. As described re claim 3, Chen discloses identifying a suspected malware file, which is a pestware object, based on data within the log files. *Id*. at ¶423. As described re claim 4, Piccard teaches analyzing the file identified by a malware detection device including whether or not the file acts suspiciously, and a POSITA would have understood that only a file that is executing (i.e., is a process) is capable of suspicious activities, and the activities of the executing process would

be recording in the consolidate log file described in Chen. EX1003, ¶¶428-429; EX1006, [0020].

Therefore, a PHOSITA would have found these limitations to be disclosed by Chen in view of Piccard. *Id*. at ¶431. As shown, the Chen-Piccard combination discloses all elements recited in claim 9 from which claim 10 depends. Accordingly, claim 4 should be found invalid under 35 U.S.C. § 103 based on Chen and Piccard.

27. Claim 11

> **The system of claim 10, including: a heuristics module configured to be executed by the hardware processor and to evaluate whether the event is a suspected pestware-related event before the research portion accesses information in the at least one log that relates the event to the suspected pestware object.**

Chen discloses that research was underway to expand the ECF to use specification languages and/or pattern recognition to identify pestware from events. EX1007, 9; EX1003, ¶528. A POSITA would have understood that matching events against pattern specifications is an example of a "heuristic," and thus that a "heuristics-based detection engine" may look for behaviors commonly exhibited by malware in order to identify suspected malware. EX1003, ¶529.

Therefore, a PHOSITA would have found these limitations to be disclosed by Chen in view of Piccard. *Id*. at ¶530. As shown, the Chen-Piccard combination

discloses all elements recited in claims 9 and 10 from which claim 11 depends. Accordingly, claim 11 should be found invalid under 35 U.S.C. § 103 based on Chen and Piccard.

28. Claim 12

> **The system of claim 11, wherein the heuristics module determines that the at least one event is suspected to be pestware-related by analyzing other events in connection with the event, wherein the other events are also related to the time of interest.**

Chen discloses correlation techniques in order for the ECF to match events together:

> (ii) the incorporation into ECF of query mechanisms by which log-specific information in addition to the base information (Time, Subject, Object and Action) is queried and correlated with information from the main Canonical table and the possible use of an XML based approach to do this (this feature will expand the range of queries possible and provide a 'drill-down' functionality into the front end);

EX1006, p. 9.

A POSITA would have understood that matching events against pattern specifications is an example of a "heuristic" as a means for estimating or guessing as to the classification of anomalous events. EX1003, ¶534. A POSITA would have understood that a "heuristics-based detection engine" looks for behaviors commonly exhibited by malware in order to identify suspected malware, even

when other detection mechanisms would not have discovered it (e.g., a never-before-seen virus that does not yet have a signature in the database of an antivirus scanner). *Id*. (citing EX1015, pp.11-12). As noted re 9[e], the ECF components disclosed in Chen are executed by the hardware processor (as they are part of the software), access the file storage device of the computer, and relate the time of interest to an externally networked source of potential pestware activity. *Id*. at ¶484.

Therefore, a PHOSITA would have found these limitations to be disclosed by Chen. *Id*. at ¶535. As shown, the Chen-Piccard combination discloses all elements recited in claims 9-11 from which claim 12 depends. Accordingly, claim 12 should be found invalid under 35 U.S.C. § 103 based on Chen and Piccard.

29. Claim 13

> **The system of claim 9, wherein the at least one log includes 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.**

This claim essentially restates the limitations in claim 5 addressed above. As discussed re 1[c] and claim 2, Chen discloses activity logs, such as the Windows 2000 Security Log, as well as event logs, such as browser logs and browser cache logs. *Id*. at ¶¶434-435. Therefore, a PHOSITA would have found these limitations to be disclosed by Chen. *Id*. at ¶431. As shown, the Chen-

Piccard combination discloses all elements recited in claim 9 from which claim 13 depends. Accordingly, claim 13 should be found invalid under 35 U.S.C. § 103 based on Chen and Piccard.

30. Claim 14

The system of claim 9, wherein the timestamp module is further configured to generate the time of interest as a point in time.

Chen discloses that the ECF Dynamic Query module issues timestamps related to suspicious events in order for the system to find all events within the time period. Specifically, Chen discloses:

> This query returned a single record from our test logs which we do not show here due to space limitations. **However, the record returned occurred at the time '2003-08-08 04:56:5' (UCT)**. The investigator would also be interested in other accounts that had been used to login to the workstation at around the same time. Therefore, in a similar fashion to the previous scenario **we perform a query to determine all the users who logged onto the workstation 'dsto' in the time window commencing ten minutes prior to the identified records**, and finishing ten minutes after it. The following SQL query, which was generated using the Dynamic Query interface, extracts the desired records:

EX1006, p. 8 (emphasis added).

> Dynamic queries are satisfied largely by access to the main database table, the Canonical table with processing of time values relying upon the field starttime in one of the two event-time related tables…
>
> When a constraint is selected, the application populates the related drop down menu with all corresponding values currently in the database and this may then be used to simply choose the desired value as the constraint. The constraints can also be set to match a sub-string. For example, if SubjectType is set to ip_address and Subject is set to "contains 131.181" then all IP addresses in the 131.181.0.0 subnet will be matched and only records satisfying that constraint will be displayed (subject to other constraints also).

EX1006, p. 4.

Chen also discloses a "point in time," identifying a "point in time" of a suspicious event on which the interval of time is based:

> The investigator would presumably be interested in knowing times when the administrator account on the workstation was logged in to. **The ECF tool Dynamic Query interface was used to generate the following query** which will return a list of records relating to logins to the 'administrator' account on the workstation in question ('dsto')…

> This query returned a single record from our test logs which we do not show here due to space limitations. However, **the record returned occurred at the time '2003-08-08 04:56:5' (UCT).**

Id. at p. 8 (emphasis added).

Therefore, a PHOSITA would have found these limitations to be disclosed by Chen. EX1003, ¶541. As shown, the Chen-Piccard combination discloses all elements recited in claim 9 from which claim 14 depends. Accordingly, claim 14 should be found invalid under 35 U.S.C. § 103 based on Chen and Piccard.

31. Claim 15

> **The system of claim 9, wherein the at least one externally networked source of potential pestware activity is identified by an identifier selected from the group consisting of an I.P. address and a URL.**

This claim is similar to claim 8 addressed above. As discussed re claim 8, Piccard discloses identifying the external network source of the potential pestware by both IP address and URL. EX1003, ¶450. Therefore, a PHOSITA would have found these limitations to be disclosed by Chen in view of Piccard. EX1003, ¶543. As shown, the Chen-Piccard combination discloses all elements recited in claim 9 from which claim 15 depends. Accordingly, claim 15 should be found invalid under 35 U.S.C. § 103 based on Chen and Piccard.

32. Claim 16

> **The system of claim 9, wherein the at least one log includes 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.**

This claim is an exact repeat of claim 13. Therefore the analysis above regarding claim 13 applies to claim 16 as well. For the same reasons as state above regarding claim 13, PHOSITA would have found these limitations to be disclosed by Chen in view of Piccard. *Id*. at ¶431. As shown, the Chen-Piccard combination discloses all elements recited in claim 9 from which claim 16 depends. Accordingly, claim 16 should be found invalid under 35 U.S.C. § 103 based on Chen and Piccard.

VI. NO BASIS FOR DISCRETIONARY DENIAL

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

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

trial is currently set for August 19, 2024. Trial is currently set for five different cases on that same date in the same Court against Webroot, of which Trend Micro's case is just one. Trial will not proceed on all five cases on the same date, and it is still unclear which, if any, parties will proceed to trial on that date and when trial would be scheduled for the remaining defendants. Thus, it is unclear the exact date Trend Micro's case will go to trial, and it is possible for this inter partes review to reach final written decision before then. Fourth, it is early in the parallel litigation as the parties are still in fact discovery, which is not set to close until January 18, 2024, after which the parties still have expert discovery, dispositive motions, and pretrial disclosures before reaching trial. Finally, Petitioner and Webroot are parties in the parallel litigation as identified in the Mandatory Notices.

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

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

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

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

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

VII. CONCLUSION

Inter partes review of claims **1-16** of U.S. Patent No. **8,181,244** is requested based on the grounds described above.

Respectfully submitted,

The Marbury Law Group, PLLC

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. 8,181,244**, Petitioner's power of attorney, and all associated exhibits were served in their entireties on September 7, 2023, on the following party via Federal Express:

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

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 **13,962** words, excluding the parts of the Petition exempted.

The Marbury Law Group, PLLC

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