

Fortinet-1002



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/428,203	09/04/2012	8261344	SPHS-0007-P01	3669

43520 7590 08/15/2012
STRATEGIC PATENTS P.C..
C/O CPA Global
P.O. BOX 52050
MINNEAPOLIS, MN 55402

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b) (application filed on or after May 29, 2000)

The Patent Term Adjustment is 1115 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (<http://pair.uspto.gov>).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site <http://pair.uspto.gov> for additional applicants):

Ben Godwood, Finstock, UNITED KINGDOM;
William James McCourt, Abingdon, UNITED KINGDOM;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

Complete if Known

Application Number	11/428,203
Filing Date	June 30, 2006
First Named Inventor	Godwood, Ben
Art Unit	Unknown
Examiner Name	Unknown

Change(s) applied
to document,

/R.K.V./

7/6/2012 (Use as many sheets as necessary)

Sheet	1	of	1	Attorney Docket No: SPHS-0007-P01
-------	---	----	---	-----------------------------------

US PATENT DOCUMENTS

Examiner Initial *	Cite No	Document Number	Publication Date	Name of Patentee or Applicant of Cited Document	Filing Date If Appropriate
/CLF/		US-20050172338	08/04/2005	Sandu, Catalin D., et al.	01/30/2004
/CLF/		US-20040181677	08/16/2004	Man-Pyo, Hong et al. 9/2004	10/30/2003

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No	Foreign Patent Document	Publication Date	Name of Patentee or Applicant of cited Document	T ²
/CLF/	A	IB-WO2006006144	01/19/2006	Zamir, Shay , et al.	

OTHER DOCUMENTS -- NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T ²
/CLF/	B	"Search Report Under Section 17(5)", <u>For Application No. GB0711866.4, mailed October 12, 2007.</u>	

EXAMINER

/Christian LaForgia/

DATE CONSIDERED

05/13/2010

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: **Mail** **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax **(571)-273-2885**

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

43520 7590 06/04/2012
STRATEGIC PATENTS P.C..
C/O CPA Global
P.O. BOX 52050
MINNEAPOLIS, MN 55402

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

John H. Nortrup	(Depositor's name)
/John H. Nortrup, Reg. No. 59,063/	(Signature)
August 1, 2012	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

11/428,203 06/30/2006 Ben Godwood SPHS-0007-P01 3669

TITLE OF INVENTION: METHOD AND SYSTEM FOR CLASSIFICATION OF SOFTWARE USING CHARACTERISTICS AND COMBINATIONS OF SUCH CHARACTERISTICS

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	\$1740	\$300	\$0	\$2040	09/04/2012

EXAMINER	ART UNIT	CLASS-SUBCLASS
LAFORGIA, CHRISTIAN A	2439	726-022000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 **Strategic Patents, P.C.**

2 _____

3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Sophos PLC

Abingdon, United Kingdom

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:

☒ Issue Fee

☒ Publication Fee (No small entity discount permitted)

☐ Advance Order - # of Copies _____

4b. Payment of Fee(s); (Please first reapply any previously paid issue fee shown above)

☐ A check is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☒ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number **50-4262** (enclose an extra copy of this form).

5. Change in Entity Status (from status indicated above)

☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.

☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature **/John H. Nortrup/**

Date **August 1, 2012**

Typed or printed name **John H. Nortrup**

Registration No. **59,063**

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

In re application of Benjamin John Godwood *et al.* : Group Art Unit: 3669
Serial No. 11/428,203 : Confirmation No. 2439
Filed: June 30, 2006 : Examiner: LAFORGIA, Christian A.

ISSUE FEE COMMUNICATION

Mail Stop Issue Fee
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Examiner:

For the above identified application, the applicant hereby authorizes the Patent Office to charge any deficiencies or credit any overpayments associated with this filing to Deposit Account No. 50-4262.

Please direct any inquiry regarding this matter to the below signed agent.

Respectfully Submitted,

STRATEGIC PATENTS, P.C.

/John Nortrup/

John H. Nortrup
Reg. No. 59,063
(207) 590-0723
Customer Number 43,520

August 1, 2012

Electronic Patent Application Fee Transmittal

Application Number:	11428203			
Filing Date:	30-Jun-2006			
Title of Invention:	METHOD AND SYSTEM FOR CLASSIFICATION OF SOFTWARE USING CHARACTERISTICS AND COMBINATIONS OF SUCH CHARACTERISTICS			
First Named Inventor/Applicant Name:	Ben Godwood			
Filer:	John H. Nortrop			
Attorney Docket Number:	SPHS-0007-P01			
Filed as Large Entity				
Utility under 35 USC 111(a) Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Utility Appl issue fee	1501	1	1740	1740
Publ. Fee- early, voluntary, or normal	1504	1	300	300

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				2040

Electronic Acknowledgement Receipt

EFS ID:	13393135
Application Number:	11428203
International Application Number:	
Confirmation Number:	3669
Title of Invention:	METHOD AND SYSTEM FOR CLASSIFICATION OF SOFTWARE USING CHARACTERISTICS AND COMBINATIONS OF SUCH CHARACTERISTICS
First Named Inventor/Applicant Name:	Ben Godwood
Customer Number:	43520
Filer:	John H. Nortrop
Filer Authorized By:	
Attorney Docket Number:	SPHS-0007-P01
Receipt Date:	01-AUG-2012
Filing Date:	30-JUN-2006
Time Stamp:	14:21:27
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$ 2040
RAM confirmation Number	723
Deposit Account	504262
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	SPHS-0007-P01_080112_IssueFeeForm.pdf	297634 172cadf540f928a4199bd85d93744a098af8afdb	no	1

Warnings:**Information:**

2	Miscellaneous Incoming Letter	SPHS-0007-P01_080112_IssueCommunication.pdf	64200 dcd4d7be84a756b1a1108b39f5d4bf93ec27cd95	no	1
---	-------------------------------	---	---	----	---

Warnings:**Information:**

3	Fee Worksheet (SB06)	fee-info.pdf	32168 e173f874597d2ba56e98a4a68a36cba6191ab27b	no	2
---	----------------------	--------------	---	----	---

Warnings:**Information:**

Total Files Size (in bytes):			394002
------------------------------	--	--	--------

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

43520 7590 06/04/2012
STRATEGIC PATENTS P.C..
C/O CPA Global
P.O. BOX 52050
MINNEAPOLIS, MN 55402

EXAMINER

LAFORGIA, CHRISTIAN A

ART UNIT

PAPER NUMBER

2439

DATE MAILED: 06/04/2012

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

11/428,203

06/30/2006

Ben Godwood

SPHS-0007-P01

3669

TITLE OF INVENTION: METHOD AND SYSTEM FOR CLASSIFICATION OF SOFTWARE USING CHARACTERISTICS AND COMBINATIONS OF SUCH CHARACTERISTICS

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	\$1740	\$300	\$0	\$2040	09/04/2012

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

**Complete and send this form, together with applicable fee(s), to: Mail Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885**

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

43520 7590 06/04/2012
STRATEGIC PATENTS P.C..
C/O CPA Global
P.O. BOX 52050
MINNEAPOLIS, MN 55402

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

11/428,203	06/30/2006	Ben Godwood	SPHS-0007-P01	3669
------------	------------	-------------	---------------	------

TITLE OF INVENTION: METHOD AND SYSTEM FOR CLASSIFICATION OF SOFTWARE USING CHARACTERISTICS AND COMBINATIONS OF SUCH CHARACTERISTICS

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
-------------	--------------	---------------	---------------------	----------------------	------------------	----------

nonprovisional	NO	\$1740	\$300	\$0	\$2040	09/04/2012
----------------	----	--------	-------	-----	--------	------------

EXAMINER	ART UNIT	CLASS-SUBCLASS
----------	----------	----------------

LAFORGIA, CHRISTIAN A	2439	726-022000
-----------------------	------	------------

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

- ☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

- (1) the names of up to 3 registered patent attorneys or agents OR, alternatively, 1 _____
(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed. 2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☐ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:

- ☐ Issue Fee
☐ Publication Fee (No small entity discount permitted)
☐ Advance Order - # of Copies _____

4b. Payment of Fee(s); (Please first reapply any previously paid issue fee shown above)

- ☐ A check is enclosed.
☐ Payment by credit card. Form PTO-2038 is attached.
☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. Change in Entity Status (from status indicated above)

- ☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27. ☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/428,203	06/30/2006	Ben Godwood	SPHS-0007-P01	3669

43520 7590 06/04/2012
STRATEGIC PATENTS P.C..
C/O CPA Global
P.O. BOX 52050
MINNEAPOLIS, MN 55402

EXAMINER

LAFORGIA, CHRISTIAN A

ART UNIT	PAPER NUMBER
----------	--------------

2439

DATE MAILED: 06/04/2012

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b) (application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 728 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 728 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (<http://pair.uspto.gov>).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No.	Applicant(s)	
	11/428,203	GODWOOD ET AL.	
	Examiner	Art Unit	
	Christian LaForgia	2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 03 April 2012.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on ____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are 1-18 and 34-36.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. ____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: ____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
 6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date ____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date ____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).**
7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

- | | |
|--|--|
| <ol style="list-style-type: none"> 1. <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) 2. <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) 3. <input checked="" type="checkbox"/> Information Disclosure Statements (PTO/SB/08),
Paper No./Mail Date <u>4/16/12</u> 4. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit
of Biological Material | <ol style="list-style-type: none"> 5. <input type="checkbox"/> Notice of Informal Patent Application 6. <input type="checkbox"/> Interview Summary (PTO-413),
Paper No./Mail Date ____. 7. <input type="checkbox"/> Examiner's Amendment/Comment 8. <input checked="" type="checkbox"/> Examiner's Statement of Reasons for Allowance 9. <input type="checkbox"/> Other ____. |
|--|--|

/Christian LaForgia/
Primary Examiner, Art Unit 2439

DETAILED ACTION

1. The amendment of 03 April 2012 is noted and made of record.
2. Claims 1-18 and 34-36 have been presented for examination.
3. Claims 19-33 have been cancelled as per Applicant's amendment.

Response to Arguments

4. Applicant's arguments, see pages 7-9, filed 03 April 2012, with respect to the prior art rejections have been fully considered and are persuasive. The prior art rejection of claims 1-18 and 34-36 has been withdrawn.

Information Disclosure Statement

5. The information disclosure statement (IDS) submitted on 16 April 2012 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Allowable Subject Matter

6. Claims 1-18 and 34-36 are allowed.
7. The following is an examiner's statement of reasons for allowance:

As noted above, the Examiner agrees with the Applicant's arguments that the prior art does not teach or disclose "identifying one or more genes each describing one or more of the at least one functional block and the at least one property of the software as a sequence of APIs and strings." The Examiner was unable to find any teaching, suggestions, or motivation that would render the limitation obvious or yield a predictable result.
8. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue

Art Unit: 2439

fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian LaForgia whose telephone number is (571)272-3792.

The examiner can normally be reached on Monday thru Thursday 7-5.

10. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad can be reached on (571) 272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

11. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christian LaForgia/
Primary Examiner, Art Unit 2439

Notice of References Cited	Application/Control No. 11/428,203	Applicant(s)/Patent Under Reexamination GODWOOD ET AL.	
	Examiner Christian LaForgia	Art Unit 2439	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2003/0110385 A1	06-2003	Golobrodsky et al.	713/188
*	B	US-2006/0123480 A1	06-2006	Oh et al.	726/023
*	C	US-7,080,355 B2	07-2006	Carlson et al.	717/120
*	D	US-2007/0239993 A1	10-2007	Sokolsky et al.	713/188
*	E	US-7,640,587 B2	12-2009	Fox et al.	726/24
*	F	US-7,725,735 B2	05-2010	Fox et al.	713/188
*	G	US-8,161,548 B1	04-2012	Wan, Justin	726/22
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11/428,203
	Filing Date	Jun 30, 2006
	First Named Inventor	Benjamin John Godwood
	Art Unit	2439
	Examiner Name	LAFORGIA, Christian A.
Sheet 1 of 3	Attorney Docket No.	SPHS-0007-P01

U.S. PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
/C.L.F./		US-8108315		Jan 31, 2012	Krawetz, Neal	
/C.L.F./		US-8069435		Nov 29, 2011	Lai, Ray Y.	
/C.L.F./		US-7398553		Jul 8, 2008	Li, Jianghao	

U.S. PATENT APPLICATION PUBLICATIONS						
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
/C.L.F./		US-2009/0328011		Dec 31, 2009	Lifliand et al.	
/C.L.F./		US-2009/0019426		Jan 15, 2009	Baeumer et al.	
/C.L.F./		US-2007/0033659		Feb 8, 2007	Hoche et al.	
/C.L.F./		US-2005/0044197		Feb 24, 2005	Lai, Ray Y.	

FOREIGN PATENT DOCUMENTS								
Examiner Initial*	Cite No	Foreign Document Number ³	Cnty Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵

NON-PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
/C.L.F./	NPL-17	DIG, DANNY et al., "Automated Detection of Refactorings in Evolving Components", Springer-Verlag Berlin. Heidelberg. 2006 , 404-428	
/C.L.F./	NPL-18	, "Application Serial No. 12/413,823 (Atty Ref SPHS-0031-P01), Non-Final Office Action mailed 3/19/2012", , 19	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11/428,203
	Filing Date	Jun 30, 2006
	First Named Inventor	Benjamin John Godwood
	Art Unit	2439
	Examiner Name	LAFORGIA, Christian A.
Sheet 2 of 3	Attorney Docket No.	SPHS-0007-P01

EXAMINER SIGNATURE			
Examiner Signature	/Christian LaForgia/	Date Considered	05/22/2012
*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.			
<small>¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.</small>			

CERTIFICATION STATEMENT			
Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):			
<input type="checkbox"/> That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e) (1).			
OR			
<input type="checkbox"/> That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e) (2).			
<input type="checkbox"/> See attached certification statement.			
<input type="checkbox"/> Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.			
<input checked="" type="checkbox"/> Applicant believes that no fees are required with this filing. However, if an Office Action on the merits has been mailed, or a fee is otherwise required, the Commissioner is hereby authorized to charge any fees due under 37 C.F.R. §§1.16 or 1.17, or to credit any overpayments, to Deposit Account No. 50-4262 in order to have this information disclosure statement considered.			
SIGNATURE			
A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.			
Signature	/Robert Mazzaresse/	Date (YYYY-MM-DD)	2012-04-16
Name/Print	Robert A. Mazzaresse	Registration Number	42,852

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11/428,203
	Filing Date	Jun 30, 2006
	First Named Inventor	Benjamin John Godwood
	Art Unit	2439
	Examiner Name	LAFORGIA, Christian A.
Sheet 3 of 3	Attorney Docket No.	SPHS-0007-P01

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**




UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
 United States Patent and Trademark Office
 Address: COMMISSIONER FOR PATENTS
 P.O. Box 1450
 Alexandria, Virginia 22313-1450
 www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 3669

SERIAL NUMBER 11/428,203	FILING or 371(c) DATE 06/30/2006 RULE	CLASS 726	GROUP ART UNIT 2439	ATTORNEY DOCKET NO. SPHS-0007-P01		
APPLICANTS Ben Godwood, Finstock, UNITED KINGDOM; William James McCourt, Abingdon, UNITED KINGDOM; ** CONTINUING DATA ***** ** FOREIGN APPLICATIONS ***** ** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ** 07/25/2006						
Foreign Priority claimed <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No 35 USC 119(a-d) conditions met <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No Verified and /CHRISTIAN A LAFORGIA/ Acknowledged Examiner's Signature		<input type="checkbox"/> Met after Allowance Initials	STATE OR COUNTRY UNITED KINGDOM	SHEETS DRAWINGS 3	TOTAL CLAIMS 33	INDEPENDENT CLAIMS 3
ADDRESS STRATEGIC PATENTS P.C.. C/O CPA Global P.O. BOX 52050 MINNEAPOLIS, MN 55402 UNITED STATES						
TITLE METHOD AND SYSTEM FOR CLASSIFICATION OF SOFTWARE USING CHARACTERISTICS AND COMBINATIONS OF SUCH CHARACTERISTICS						
FILING FEE RECEIVED 1780	FEES: Authority has been given in Paper No. _____ to charge/credit DEPOSIT ACCOUNT No. _____ for following:		<input type="checkbox"/> All Fees <input type="checkbox"/> 1.16 Fees (Filing) <input type="checkbox"/> 1.17 Fees (Processing Ext. of time) <input type="checkbox"/> 1.18 Fees (Issue) <input type="checkbox"/> Other _____ <input type="checkbox"/> Credit			

<i>Index of Claims</i> 	Application/Control No. 11428203	Applicant(s)/Patent Under Reexamination GODWOOD ET AL.
	Examiner Christian LaForgia	Art Unit 2439

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

<input type="checkbox"/> Claims renumbered in the same order as presented by applicant						<input type="checkbox"/> CPA		<input type="checkbox"/> T.D.		<input type="checkbox"/> R.1.47	
CLAIM		DATE									
Final	Original	05/14/2010	03/07/2011	09/28/2011	05/23/2012						
1	1	✓	✓	✓	=						
2	2	✓	✓	✓	=						
3	3	✓	✓	✓	=						
4	4	✓	✓	✓	=						
5	5	✓	✓	✓	=						
6	6	✓	✓	✓	=						
7	7	✓	✓	✓	=						
8	8	✓	✓	✓	=						
9	9	✓	✓	✓	=						
10	10	✓	✓	✓	=						
11	11	✓	✓	✓	=						
12	12	✓	✓	✓	=						
13	13	✓	✓	✓	=						
14	14	✓	✓	✓	=						
15	15	✓	✓	✓	=						
16	16	✓	✓	✓	=						
17	17	✓	✓	✓	=						
18	18	✓	✓	✓	=						
	19	✓	✓	✓	-						
	20	✓	✓	✓	-						
	21	✓	✓	✓	-						
	22	✓	✓	✓	-						
	23	✓	✓	✓	-						
	24	✓	✓	✓	-						
	25	✓	✓	✓	-						
	26	✓	✓	✓	-						
	27	✓	✓	✓	-						
	28	✓	✓	✓	-						
	29	✓	✓	✓	-						
	30	✓	✓	✓	-						
	31	✓	✓	✓	-						
	32	✓	✓	✓	-						
	33	✓	✓	✓	-						
19	34				=						
20	35				=						
21	36				=						

EAST Search History

EAST Search History (Prior Art)


Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	0	(gene with API with string).clm.	US-PGPUB; USPAT	OR	ON	2012/05/23 09:33
S1	3	sophos.as.	US-PGPUB; USPAT	OR	ON	2010/05/13 09:11
S2	3	godwood-ben\$.in.	US-PGPUB; USPAT	OR	ON	2010/05/13 09:11
S3	4	mccourt-william\$.in.	US-PGPUB; USPAT	OR	ON	2010/05/13 09:14
S4	2	("20050172338" "20040181677").pn.	US-PGPUB; USPAT	OR	ON	2010/05/13 09:16
S5	5	("2005/0172338").URPN.	USPAT	OR	OFF	2010/05/13 09:21
S6	0	("2004/0181677").URPN.	USPAT	OR	OFF	2010/05/13 09:22
S7	0	("2004/0181677").URPN.	USPAT	OR	OFF	2010/05/13 09:22
S8	1	(anti\$virus (malware virus trojan adware spyware dialer) near detect\$3) same (detect\$3 determin\$5) with (malware malicious trojan adware spyware dialer) with (decompil\$3 disassembl\$3) with (program code)	US-PGPUB; USPAT	OR	ON	2010/05/13 09:25
S9	8	(detect\$3 determin\$5) with (malware malicious trojan adware spyware dialer) with (decompil\$3 disassembl\$3) with (program code)	US-PGPUB; USPAT	OR	ON	2010/05/13 09:27
S10	63	(detect\$3 determin\$5) with (malware malicious trojan adware spyware dialer) with (characteristic) with (program code)	US-PGPUB; USPAT	OR	ON	2010/05/13 09:30
S11	8	(detect\$3 determin\$5) with (malware malicious trojan adware spyware dialer) with (characteristic) with (program code) and (disassembl\$3 unpack\$3)	US-PGPUB; USPAT	OR	ON	2010/05/13 09:31
S13	3	("2006/0123244").URPN.	USPAT	OR	OFF	2010/05/13 11:20
S14	11	((("20050005153") or ("20040041315") or ("5381533") or ("5765030") or ("20020091934") or ("6704925") or ("5826013") or ("5951698") or ("6357008") or ("20030101381") or ("6637514"))).PN.	US-PGPUB; USPAT	OR	OFF	2010/05/13 11:28
S15	77	("6357008").URPN.	USPAT	OR	OFF	2010/05/13 11:30
S16	74	("5826013").URPN.	USPAT	OR	OFF	2010/05/13 11:38
S17	1	(US-20060123244-\$).did.	US-PGPUB	OR	OFF	2010/05/13

						12:22
S18	1	S17 and quarantin\$3	US-PGPUB; USPAT	OR	ON	2010/05/13 12:22
S19	18	726/24.ccls. and program with API near call	US-PGPUB; USPAT	OR	OFF	2011/03/07 11:49
S20	29	(scan\$4 check\$3 determin\$5 detect\$3) with API near call with (malware malicious virus trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2011/03/07 11:52
S21	3	("20040181677" "20050172338" "20090187992").pn.	US-PGPUB; USPAT	OR	OFF	2011/03/07 12:04
S22	13	726/24.ccls. and gene	US-PGPUB; USPAT	OR	ON	2011/03/07 12:06
S23	1	(US-20060123244-\$).did.	US-PGPUB	OR	OFF	2011/03/07 12:56
S24	1	S23 and basic adj block	US-PGPUB; USPAT	OR	ON	2011/03/07 12:56
S25	5387	726/22-24.ccls.	US-PGPUB; USPAT	OR	OFF	2011/09/27 14:05
S26	5	726/22-24.ccls. and basic near block with (property function\$6)	US-PGPUB; USPAT	OR	ON	2011/09/27 14:06
S27	0	(monitor\$3 scan\$4) with basic near block with (property function\$6) with (detect\$3 determin\$5 check\$3) near3 (malware malicious virus trojan spy\$ware ad\$ware)	US-PGPUB; USPAT	OR	ON	2011/09/27 14:08
S28	2	(monitor\$3 scan\$4) with basic near block with (property function\$6) same (detect\$3 determin\$5 check\$3) near3 (malware malicious virus trojan spy\$ware ad\$ware)	US-PGPUB; USPAT	OR	ON	2011/09/27 14:08
S29	0	basic near block with (property function\$6) with (detect\$3 determin\$5 check\$3) near3 (malware malicious virus trojan spy\$ware ad\$ware)	US-PGPUB; USPAT	OR	ON	2011/09/27 14:11
S30	2	basic near block with (property function\$6) same (detect\$3 determin\$5 check\$3) near3 (malware malicious virus trojan spy\$ware ad\$ware)	US-PGPUB; USPAT	OR	ON	2011/09/27 14:13
S31	2	basic near block with (property function\$6) same (detect\$3 determin\$5 check\$3) near3 (malware malicious virus trojan spy\$ware ad\$ware)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/09/27 14:13
S32	156	S25 and "717".clas.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/09/27 14:14
S33	7	S25 and "717".clas. and basic near block	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/09/27 14:14
S34	0	(monitor\$3 scan\$4) with basic near block with heuristic\$4	US-PGPUB; USPAT	OR	ON	2011/09/27 14:30
S35	1	(monitor\$3 scan\$4) with (basic code) near2 block with heuristic\$4	US-PGPUB; USPAT	OR	ON	2011/09/27 14:30

S36	21	(monitor\$3 scan\$4 detect\$3 determin\$5) with (basic code) near2 block with heuristic\$4	US-PGPUB; USPAT	OR	ON	2011/09/27 14:31
S37	1	(monitor\$3 scan\$4 detect\$3 determin\$5) with (basic code) near2 block with heuristic\$4 and "726".clas.	US-PGPUB; USPAT	OR	ON	2011/09/27 14:31
S38	5387	726/22-24.ccls.	US-PGPUB; USPAT	OR	OFF	2011/09/27 14:32
S39	5387	S38	US-PGPUB; USPAT	OR	ON	2011/09/27 14:32
S40	48	S39 and gene	US-PGPUB; USPAT	OR	ON	2011/09/27 14:32
S41	1	"20080040710".pn.	US-PGPUB; USPAT	OR	ON	2011/09/27 14:38
S42	0	S39 and gene	EPO	OR	ON	2011/09/27 14:41
S43	2	("2008/0040710").URPN.	USPAT	OR	OFF	2011/09/27 14:42
S44	0	("7996904").URPN.	USPAT	OR	OFF	2011/09/27 14:42
S45	1	"20080040710".pn.	US-PGPUB; USPAT	OR	ON	2011/09/27 16:25
S46	0	S45 and notif\$7	US-PGPUB; USPAT	OR	ON	2011/09/27 16:25
S47	0	S45 and alert\$3	US-PGPUB; USPAT	OR	ON	2011/09/27 16:25
S48	1	S45 and unpack\$3	US-PGPUB; USPAT	OR	OFF	2011/09/27 16:30
S49	0	S45 and filter\$3	US-PGPUB; USPAT	OR	OFF	2011/09/27 16:31
S50	1	S45 and translat\$3	US-PGPUB; USPAT	OR	OFF	2011/09/27 16:32
S51	0	S45 and unencrypt\$3	US-PGPUB; USPAT	OR	OFF	2011/09/27 16:33
S52	1	S45 and decrypt\$3	US-PGPUB; USPAT	OR	OFF	2011/09/27 16:33
S53	5	("8108315" "8069435" "7398553" "20090328011" "2007003659" "20050044197").pn.	US-PGPUB; USPAT	OR	OFF	2012/05/03 15:59
S54	15	("7398553").URPN.	USPAT	OR	OFF	2012/05/03 16:03
S55	41	("20020188608" "20030101144" "20030221116" "20040153994" "20040177088" "20040199594" "20040264696" "20050015758" "20050065970" "20050172338" "20050216898" "20050278259" "20060064682" "20060116966" "20060129523" "20060136867" "20060212464" "20060277531" "20070088740" "20070260651" "20070261038" "20080091938" "3711863" "5937084" "5974254" "6145124" "6199201" "6282698" "6748584" "7080037" "7100195" "7210041" "7296261" "7359948" "7398553" "7421418" "7500222"	US-PGPUB; USPAT; USOCR	OR	OFF	2012/05/22 09:58

		"7503035" "7542958" "7707634" "7797245").PN.				
S56	7	("8108315" "8069435" "7398553" "20090328011" "20090019426" "20070033659" "20050044197").pn.	US-PGPUB; USPAT; USOCR	OR	OFF	2012/05/22 10:03
S57	15	("7398553").URPN.	USPAT	OR	OFF	2012/05/22 10:05
S58	675	(726/22-25.ccls. and 713/188.ccls.)	US-PGPUB; USPAT	OR	OFF	2012/05/22 10:28
S59	675	(726/22-25.ccls. and 713/188.ccls.)	US-PGPUB; USPAT	OR	ON	2012/05/22 10:28
S60	7111	(726/22-25.ccls. 713/188.ccls.)	US-PGPUB; USPAT	OR	ON	2012/05/22 10:28
S61	57	(726/22-25.ccls. 713/188.ccls.) and genes	US-PGPUB; USPAT	OR	ON	2012/05/22 10:28
S62	5254	(726/22-25.ccls. 713/188.ccls.) and gene\$3	US-PGPUB; USPAT	OR	ON	2012/05/22 10:29
S63	148	(726/22-25.ccls. 713/188.ccls.) and (gene genetic)	US-PGPUB; USPAT	OR	ON	2012/05/22 10:29
S64	2	("2003/0110385").URPN.	USPAT	OR	OFF	2012/05/22 11:00
S65	1498	717/126-127.ccls.	USPAT	OR	OFF	2012/05/22 11:27
S66	50	S60 and S65	USPAT	OR	OFF	2012/05/22 11:27
S67	50	S60 and S65	US-PGPUB; USPAT	OR	OFF	2012/05/22 11:27
S68	781	717/131.ccls.	USPAT	OR	OFF	2012/05/22 11:29
S69	14	S68 and S60	USPAT	OR	OFF	2012/05/22 11:29
S70	291372	classif\$7	USPAT	OR	ON	2012/05/22 11:31
S71	4302	classif\$7 with (code soft\$ware program) with (function\$5 property)	US-PGPUB; USPAT	OR	ON	2012/05/22 11:31
S72	1369	classif\$7 near3 (code soft\$ware program) with (function\$5 property)	US-PGPUB; USPAT	OR	ON	2012/05/22 11:31
S73	11	classif\$7 near3 (code soft\$ware program) with function\$5 with property	US-PGPUB; USPAT	OR	ON	2012/05/22 11:32
S74	29	classif\$7 near3 (code soft\$ware program) with (function\$5 property) with (API string)	US-PGPUB; USPAT	OR	ON	2012/05/22 11:33

5/ 23/ 2012 9:33:56 AM
C:\ Users\ claforgia\ Documents\ EAST\ Workspaces\ 11428203.wsp

Search Notes 	Application/Control No. 11428203	Applicant(s)/Patent Under Reexamination GODWOOD ET AL.
	Examiner Christian LaForgia	Art Unit 2439

SEARCHED			
Class	Subclass	Date	Examiner
none	none	5/13/10	clf
726	24	3/7/11	clf
726	22-24	9/27/11	clf
726	22-25	5/22/12	clf
713	188	5/22/12	clf
717	126, 127, 131	5/22/12	clf

SEARCH NOTES		
Search Notes	Date	Examiner
EAST search - see enclosed	5/13/10	clf
IEEE search	5/13/10	clf
ACM search	5/13/10	clf
Google search	5/13/10	clf
Inventor search	5/13/10	clf
Assignee search	5/13/10	clf
updated EAST - see enclosed	3/7/11	clf
updated EAST - see enclosed	9/27/11	clf
updated EAST - see enclosed	5/22/12	clf

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner
	(gene with API with string).clm.	5/23/12	clf

	/Christian LaForgia/ Primary Examiner.Art Unit 2439
--	--

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11/428,203
	Filing Date	Jun 30, 2006
	First Named Inventor	Benjamin John Godwood
	Art Unit	2439
	Examiner Name	LAFORGIA, Christian A.
Sheet 1 of 3	Attorney Docket No.	SPHS-0007-P01

U.S. PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-8108315		Jan 31, 2012	Krawetz, Neal	
		US-8069435		Nov 29, 2011	Lai, Ray Y.	
		US-7398553		Jul 8, 2008	Li, Jianghao	

U.S. PATENT APPLICATION PUBLICATIONS						
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-2009/0328011		Dec 31, 2009	Lifliand et al.	
		US-2009/0019426		Jan 15, 2009	Baeumer et al.	
		US-2007/0033659		Feb 8, 2007	Hoche et al.	
		US-2005/0044197		Feb 24, 2005	Lai, Ray Y.	

FOREIGN PATENT DOCUMENTS								
Examiner Initial*	Cite No	Foreign Document Number ³	Cnty Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵

NON-PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	NPL-17	DIG, DANNY et al., "Automated Detection of Refactorings in Evolving Components", Springer-Verlag Berlin. Heidelberg. 2006 , 404-428	
	NPL-18	, "Application Serial No. 12/413,823 (Atty Ref SPHS-0031-P01), Non-Final Office Action mailed 3/19/2012", , 19	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11/428,203
	Filing Date	Jun 30, 2006
	First Named Inventor	Benjamin John Godwood
	Art Unit	2439
	Examiner Name	LAFORGIA, Christian A.
Sheet 2 of 3	Attorney Docket No.	SPHS-0007-P01

EXAMINER SIGNATURE			
Examiner Signature		Date Considered	
*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.			
<small>¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.</small>			

CERTIFICATION STATEMENT			
Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):			
<input type="checkbox"/> That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e) (1).			
OR			
<input type="checkbox"/> That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e) (2).			
<input type="checkbox"/> See attached certification statement.			
<input type="checkbox"/> Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.			
<input checked="" type="checkbox"/> Applicant believes that no fees are required with this filing. However, if an Office Action on the merits has been mailed, or a fee is otherwise required, the Commissioner is hereby authorized to charge any fees due under 37 C.F.R. §§1.16 or 1.17, or to credit any overpayments, to Deposit Account No. 50-4262 in order to have this information disclosure statement considered.			
SIGNATURE			
A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.			
Signature	/Robert Mazzaresse/	Date (YYYY-MM-DD)	2012-04-16
Name/Print	Robert A. Mazzaresse	Registration Number	42,852

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11/428,203
	Filing Date	Jun 30, 2006
	First Named Inventor	Benjamin John Godwood
	Art Unit	2439
	Examiner Name	LAFORGIA, Christian A.
Sheet 3 of 3	Attorney Docket No.	SPHS-0007-P01

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/413,823	03/30/2009	Robert J. Poston	SPHS-0031-P01	9870

43520 7590 03/19/2012
STRATEGIC PATENTS P.C..
C/O CPA Global
P.O. BOX 52050
MINNEAPOLIS, MN 55402

EXAMINER

LAFORGIA, CHRISTIAN A

ART UNIT	PAPER NUMBER
----------	--------------

2439

NOTIFICATION DATE	DELIVERY MODE
-------------------	---------------

03/19/2012

ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@cpaglobal.com

Office Action Summary	Application No.	Applicant(s)	
	12/413,823	POSTON, ROBERT J.	
	Examiner	Art Unit	
	Christian LaForgia	2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 30 March 2009.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on ____; the restriction requirement and election have been incorporated into this action.
- 4) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 5) ☒ Claim(s) 1-24 is/are pending in the application.
- 5a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 6) ☐ Claim(s) ____ is/are allowed.
- 7) ☒ Claim(s) 1-24 is/are rejected.
- 8) ☐ Claim(s) ____ is/are objected to.
- 9) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 10) ☐ The specification is objected to by the Examiner.
- 11) ☒ The drawing(s) filed on 30 March 2009 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 12) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. ____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. ____. |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date <u>8/18/10;5/17/11;12/5/11</u> . | 6) <input type="checkbox"/> Other: ____. |

DETAILED ACTION

1. Claims 1-24 have been presented for examination.

Priority

2. Acknowledgment is made of applicant's claim as a continuation-in-part of application no. 11/428,203.

Information Disclosure Statement

3. The information disclosure statements (IDS) submitted on 18 August 2010, 17 May 2011, and 05 December 2011 are in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statements have been considered by the examiner.

Claim Objections

4. Applicant is advised that should claims 6-11 be found allowable, claims 18-23 will be objected to under 37 CFR 1.75 as being a substantial duplicate thereof. When two claims in an application are duplicates or else are so close in content that they both cover the same thing, despite a slight difference in wording, it is proper after allowing one claim to object to the other as being a substantial duplicate of the allowed claim. See MPEP § 706.03(k). For the purposes of examination, the Examiner will interpret claims 18 and 19 as depending from claim 12.

Claim Rejections - 35 USC § 101

5. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

6. Claims 1-24 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 1-24 are directed to “[a] computer program product embodied in a computer-readable medium” Paragraphs 0092 and 0094 disclose the use of

Art Unit: 2439

wired and wireless media, such that one of ordinary skill in the art could reasonably construe the claimed computer-readable medium as including both storage media and transmission media.

The Office's current position is that claims involving transmission media, such as signals encoded with functional descriptive material, do not fall within any of the categories of patentable subject matter set forth in 35 U.S.C. § 101, and such claims are therefore ineligible for patent protection. *In re Nuijten*, 500 F.3d 1346, 1357 (Fed. Cir. 2007), *reh'g en banc denied*, 515 F.3d 1361 (Fed. Cir. 2008), *cert. denied*, 129 S.Ct. 70 (2008). The Office's preferred claim language is "A non-transitory computer readable medium comprising a computer program product"

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

8. Claims 1-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 8,108,315 B2 to Krawetz, hereinafter Krawetz, in view of U.S. Patent No. 7,398,553 B1 to Li, hereinafter Li.

9. As per claim 1, Krawetz teaches a computer program product embodied in a computer readable medium that, when executing on one or more computers, performs the steps of:

a. identifying a functional code block that performs a particular function within executable code (Figure 1 [step 120], column 3, lines 23-32);

Art Unit: 2439

b. transforming the functional code block into a generic code representation of its functionality by tokenizing the functional code block (Figure 1 [step 140], column 3, line 40-61);

c. comparing the generic code representation with a previously characterized functions (Figure 1 [step 150], column 3, line 62 to column 4, line 24); and

d. determining if there is a positive correlation based on the comparison (Figure 1 [step 160], column 4, lines 25-35).

10. Krawetz does not teach wherein the previously characterized functions are malicious code representations, and in response to a positive correlation from the comparison, identifying the executable code as containing malicious code.

11. Li teaches comparing the generic code representation with a previously characterized malicious code representation (Figures 3 [item 218], 4 [step 312], column 7, line to column 8, line 7, column 10, lines 5-21), and

in response to a positive correlation from the comparison, identifying the executable code as containing malicious code (Figures 3 [item 220], 4 [step 314], column 7, lines 47-51, column 10, lines 16-21).

12. It would have been obvious to one of ordinary skill in the art at the time the invention was made to add the virus scanning capabilities of Li to the system of Krawetz, since Li states at column 3, lines 1-16 that comparing tokenized versions of code and/or scripts provides a better methodology for detecting viruses and their polymorphs.

13. Regarding claim 2, Krawetz teaches wherein tokenization eliminates portions in the functional code block that may be presented in differing versions of code that perform the same

Art Unit: 2439

function as the functional code block (Figures 1 [step 140], and associated written descriptions, as well as column 3, line 40-61. *See also* Li, Figure 9B and associated written descriptions.).

14. With regards to claim 3, Krawetz teaches wherein the eliminated portions occur as a result of changed cross references due to variations in content and location of code between the differing versions (Figures 1 [step 140], and associated written descriptions, as well as column 3, line 40-61. *See also* Li, Figure 9B and associated written descriptions.).

15. With regards to claim 4, Krawetz teaches wherein the differences occur as a result of legitimate optimization techniques (Figure 1 [step 140], column 3, line 40-61).

16. With regards to claim 5, Li teaches wherein the differences occur as a result of malicious obfuscation techniques (column 3, lines 1-16, i.e. polymorphic viruses changing code).

17. Regarding claim 6, Krawetz and Li teach wherein the executable code is at least one of executable software, a script, a byte code file, and machine code (Krawetz: Figure 1 [step 110], column 2, lines 56-67; Li: Figure 3 [items 202, 204, 204'], column 6, lines 4-13).

18. Regarding claim 7, Li teaches wherein the malicious code representation is pulled from a library of malicious code representations (Figures 2 [item 108], 3 [item 214], column 2, lines 25-38, column 7, lines 43-51, pattern file database).

Art Unit: 2439

19. With regards to claim 8, Li teaches wherein the library is stored on the computer performing a local code scan (Figures 2 [item 108], 3 [item 214], column 2, lines 25-38, column 7, lines 43-51, pattern file database). One of ordinary skill in the art would recognize that the virus signature database could be implemented locally on the machine implementing the scan and Official Notice is taken of such.

20. With regards to claim 9, Li teaches wherein the library is accessed through a network (Figures 2 [item 108], 3 [item 214], column 2, lines 25-38, column 7, lines 43-51, pattern file database). One of ordinary skill in the art would recognize that the virus signature database could be implemented over a network and Official Notice is taken of such.

21. With regards to claim 10, Li teaches wherein the library is accessed through a threat research center (Figure 3 [items 212, 222], column 6, line 62 to column 7, line 42).

22. With regards to claim 11, Li teaches wherein the library is updated from a threat research center (Figure 3 [items 212, 222], column 6, line 62 to column 7, line 42).

23. As per claim 12, Krawetz teaches a computer program product embodied in a computer readable medium that, when executing on one or more computers, performs the steps of:

a. identifying a functional code block that performs a particular function within executable code (Figure 1 [step 120], column 3, lines 23-32);

Art Unit: 2439

b. transforming the functional code block into a generic code representation of its functionality by refactoring the functional code block (Figure 1 [step 130], column 3, lines 31-39, column 3, lines 49-61. According to **Automated Detection of Refactorings in Evolving Components**, examples of refactoring include “changing the names of classes and methods, moving methods and fields from one class to another, and splitting methods or classes.” Krawetz discloses the replacing of generic terms in each function thereby performing the refactoring of changing the names of classes and methods.);

c. comparing the generic code representation with a previously characterized functions (Figure 1 [step 150], column 3, line 62 to column 4, line 24); and

d. determining if there is a positive correlation based on the comparison (Figure 1 [step 160], column 4, lines 25-35).

24. Krawetz does not teach wherein the previously characterized functions are malicious code representations, and in response to a positive correlation from the comparison, identifying the executable code as containing malicious code.

25. Li teaches comparing the generic code representation with a previously characterized malicious code representation (Figures 3 [item 218], 4 [step 312], column 7, line to column 8, line 7, column 10, lines 5-21), and

in response to a positive correlation from the comparison, identifying the executable code as containing malicious code (Figures 3 [item 220], 4 [step 314], column 7, lines 47-51, column 10, lines 16-21).

26. It would have been obvious to one of ordinary skill in the art at the time the invention was made to add the virus scanning capabilities of Li to the system of Krawetz, since Li states at

Art Unit: 2439

column 3, lines 1-16 that comparing tokenized versions of code and/or scripts provides a better methodology for detecting viruses and their polymorphs.

27. Regarding claim 13, Krawetz teaches wherein refactoring eliminates portions in the functional code block that may be presented in differing versions of code that perform the same function as the functional code block (Figure 1 [step 130], column 3, lines 31-39, column 3, lines 49-61).

28. With regards to claim 14, Krawetz teaches wherein the eliminated portions occur as a result of changed cross references due to variations in content and location of code between the differing versions (Figure 1 [step 130], column 3, lines 31-39, column 3, lines 49-61).

29. With regards to claim 15, Krawetz teaches wherein the differences occur as a result of legitimate optimization techniques (Figure 1 [step 130], column 3, lines 31-39, column 3, lines 49-61).

30. With regards to claim 16, Li teaches wherein the differences occur as a result of malicious obfuscation techniques (column 3, lines 1-16, i.e. polymorphic viruses changing code).

31. With regards to claim 17, Krawetz teaches wherein the refactoring is lossy refactoring which selectively preserves certain generic characteristics of the code without needing to maintain actual executability (Figure 1 [step 130], column 3, lines 31-39, column 3, lines 49-61).

Art Unit: 2439

32. Regarding claim 18, both Krawetz & Li teach wherein the executable code is at least one of executable software, a script, a byte code file, and machine code (Krawetz: Figure 1 [step 110], column 2, lines 56-67; Li: Figure 3 [items 202, 204, 204'], column 6, lines 4-13).

33. Regarding claim 19, Li teaches wherein the malicious code representation is pulled from a library of malicious code representations (Figures 2 [item 108], 3 [item 214], column 2, lines 25-38, column 7, lines 43-51, pattern file database).

34. With regards to claim 20, Li teaches wherein the library is stored on the computer performing a local code scan (Figures 2 [item 108], 3 [item 214], column 2, lines 25-38, column 7, lines 43-51, pattern file database). One of ordinary skill in the art would recognize that the virus signature database could be implemented locally on the machine implementing the scan and Official Notice is taken of such.

35. With regards to claim 21, Li teaches wherein the library is accessed through a network (Figures 2 [item 108], 3 [item 214], column 2, lines 25-38, column 7, lines 43-51, pattern file database). One of ordinary skill in the art would recognize that the virus signature database could be implemented over a network and Official Notice is taken of such.

36. With regards to claim 22, Li teaches wherein the library is accessed through a threat research center (Figure 3 [items 212, 222], column 6, line 62 to column 7, line 42).

Art Unit: 2439

37. With regards to claim 23, Li teaches wherein the library is updated from a threat research center (Figure 3 [items 212, 222], column 6, line 62 to column 7, line 42).

38. As per claim 24, Krawetz teaches a computer program product embodied in a computer readable medium that, when executing on one or more computers, performs the steps of:

a. identifying a plurality of functional code blocks within executable code (Figure 1 [step 120], column 3, lines 23-32);

b. transforming the plurality of functional code blocks into a plurality of generic code representations of its functionality by at least one of refactoring and tokenizing the plurality of functional code blocks (Figure 1 [steps 130, 140], column 3, line 31-61);

c. comparing the generic code representation with a previously characterized functions (Figure 1 [step 150], column 3, line 62 to column 4, line 24); and

d. determining if there is a positive correlation based on the comparison (Figure 1 [step 160], column 4, lines 25-35).

39. Krawetz does not teach wherein the previously characterized functions are malicious code representations, and in response to a positive correlation from the comparison, identifying the executable code as containing malicious code.

40. Li teaches comparing the generic code representation with a previously characterized malicious code representation (Figures 3 [item 218], 4 [step 312], column 7, line to column 8, line 7, column 10, lines 5-21), and

Art Unit: 2439

in response to a positive correlation from the comparison, identifying the executable code as containing malicious code (Figures 3 [item 220], 4 [step 314], column 7, lines 47-51, column 10, lines 16-21).

41. It would have been obvious to one of ordinary skill in the art at the time the invention was made to add the virus scanning capabilities of Li to the system of Krawetz, since Li states at column 3, lines 1-16 that comparing tokenized versions of code and/or scripts provides a better methodology for detecting viruses and their polymorphs.

Conclusion

42. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

43. The following patents are cited to further show the state of the art with respect to detecting polymorphic viruses, such as:

United States Patent Application Publication No. 2009/0328011 A1 to Lifliand et al., which is cited to show detecting malicious code using tokenization.

United States Patent Application Publication No. 2009/0019426 A1 to Baeumer et al., which is cited to show a refactoring engine that is used to help detect malware.

United States Patent Application Publication No. 2007/0033659 A1 to Hoche et al., which is cited to show using refactoring as a step in detecting malware.

United States Patent Application Publication No. 2005/0044197 A1 to Lai, which is cited to show using refactoring as a step in detecting patterns in code.

United States Patent No. 8,069,435 B1 to Lai, which is cited to show using refactoring as a step in detecting patterns in code.

Art Unit: 2439

44. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian LaForgia whose telephone number is (571)272-3792.

The examiner can normally be reached on Monday thru Thursday 7-5.

45. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad can be reached on (571) 272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

46. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christian LaForgia/
Primary Examiner, Art Unit 2439

clf

Notice of References Cited	Application/Control No. 12/413,823		Applicant(s)/Patent Under Reexamination POSTON, ROBERT J.	
	Examiner Christian LaForgia		Art Unit 2439	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2005/0044197 A1	02-2005	Lai, Ray Y.	709/223
*	B	US-2007/0033659 A1	02-2007	Hoche et al.	726/028
*	C	US-7,398,553 B1	07-2008	Li, Jianghao	726/22
*	D	US-2009/0019426 A1	01-2009	Baeumer et al.	717/122
*	E	US-2009/0328011 A1	12-2009	Lifliand et al.	717/140
*	F	US-8,069,435 B1	11-2011	Lai, Ray Y	717/106
*	G	US-8,108,315 B2	01-2012	Krawetz, Neal	705/59
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Danny Dig et al. Automated Detection of Refactorings in Evolving Components. 2006. Springer-Verlag Berlin. Heidelberg. p. 404-428.
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	12/413,823
	Filing Date	Mar 30, 2009
	First Named Inventor	Robert J. Poston
	Art Unit	2431
	Examiner Name	BARRON, Jr., Gilberto
Sheet 1 of 3	Attorney Docket No.	SPHS-0031-P01

U.S. PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
/C.L.F./		US-7814544 B1		Oct 12, 2010	Wilhelm, Jeffrey	

U.S. PATENT APPLICATION PUBLICATIONS						
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
/C.L.F./		US-20060015940A1	A8	Jan 19, 2006	Zamir, Shay et al.	
/C.L.F./		US-20050187740A1	A8	Aug 25, 2005	Marinescu, Adrian M.	

FOREIGN PATENT DOCUMENTS								
Examiner Initial*	Cite No	Foreign Document Number ³	Cnty Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵

NON-PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
/C.L.F./	NPL-10	"Application Serial No.11/428,203 (Atty Ref SPHS-0007-P01), Final Office Action mailed 03/16/2011", , 14	

/Christian LaForgia/

03/13/2012

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449A/PTO				
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>		<i>Complete if Known</i>		
		Application Number	12/413,823	
		Filing Date	Mar 30, 2009	
		First Named Inventor	Robert J. Poston	
		Art Unit	2431	
		Examiner Name	BARRON, Jr., Gilberto	
Sheet	1	of	1	Attorney Docket No: SPHS-0031-P01

US PATENT DOCUMENTS					
Examiner Initial *	Cite No	Document Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
/C.L.F./		2004/0181677	Sep 16, 2004	Hong, Man-Pyo et al.	
/C.L.F./		20040181677	Aug 16, 2004	Man-Pyo, Hong et al.	
/C.L.F./		2005/0172338	Aug 4, 2005	Sandu, Catalin D., et al.	
/C.L.F./		20050172338	Aug 4, 2005	Sandu, Catalin D., et al.	
/C.L.F./		20060123244A1	Jun 8, 2006	Gheorghescu, G. M., et al.	
/C.L.F./		20070240212A1	Oct 11, 2007	Matalytski, Siarhei	
/C.L.F./		20080010538A1	Jan 10, 2008	Satish, S. et al.	
/C.L.F./		5826013A	Oct 20, 1998	Nachenberg, C. S.	
/C.L.F./		6357008B1	Mar 12, 2002	Nachenberg, C. S.	
/C.L.F./		7013483B2	Mar 14, 2006	Cohen, O. et al.	
/C.L.F./		7069583B2	Jun 27, 2006	Yann, T. et al.	
/C.L.F./		7496963B2	Feb 24, 2009	Shipp, A.	
/C.L.F./		7519997B2	Apr 14, 2009	Shipp, A.	
/C.L.F./		7636856B2	Dec 22, 2009	Marinescu, A. M., et al.	
/C.L.F./		7636945B2	Dec 22, 2009	Chandnani, A. et al.	

FOREIGN PATENT DOCUMENTS					
Examiner Initials*	Cite No	Foreign Patent Document	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
/C.L.F./		IB-WO2006006144	Jan 19, 2006	Zamir, Shay et al.	

OTHER DOCUMENTS -- NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T ²
/C.L.F./	NPL-1	, "Application Serial No. 11/428,203(Atty Ref SPHS-0007-P01), Non-Final Office Action mailed 5-17-10", , 13	
/C.L.F./	NPL-2	, "Search Report Under Section 17(5)", <u>For Application No. GB0711866.4, mailed October 12, 2007</u>	
/C.L.F./	NPL-7	SKORMIN, et al., ""In The Search of the "Gene of Replication" in Malicious Codes"", <u>Proceedings from the Sixth Annual IEEE Systems, Man and Cybernetics Information Assurance Workshop 2005</u> , 193-200	

EXAMINER

/Christian LaForgia/

DATE CONSIDERED

03/13/2012

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	12/413,823
	Filing Date	Mar 30, 2009
	First Named Inventor	Robert J. Poston
	Art Unit	2431
	Examiner Name	TRAORE, Fatoumata
Sheet 1 of 3	Attorney Docket No.	SPHS-0031-P01

U.S. PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
/C.L.F./		US-6301699 B1		Oct 9, 2001	Hollander, Y et al.	

U.S. PATENT APPLICATION PUBLICATIONS						
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
/C.L.F./		US-2009018 7992 A1		Jul 23, 2009	Poston, R	
/C.L.F./		US-2008004 0710 A1		Feb 14, 2008	Chiriac, M	
/C.L.F./		US-2007001 6953 A1		Jan 18, 2007	Morris, M et al.	

FOREIGN PATENT DOCUMENTS								
Examiner Initial*	Cite No	Foreign Document Number ³	Cnty Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵

NON-PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
/C.L.F./	NPL-14	, "Application Serial No. 11428,203 (Atty Ref SPHS-0007-P01), Non-Final Office Action mailed 10/04/2011", , 11	

EXAMINER SIGNATURE			
Examiner Signature	/Christian LaForgia/	Date Considered	03/13/2012

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	12/413,823
	Filing Date	Mar 30, 2009
	First Named Inventor	Robert J. Poston
	Art Unit	2431
	Examiner Name	TRAORE, Fatoumata
Sheet 2 of 3	Attorney Docket No.	SPHS-0031-P01

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e) (1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e) (2).

☐ See attached certification statement.

☐ Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ Applicant believes that no fees are required with this filing. However, if an Office Action on the merits has been mailed, or a fee is otherwise required, the Commissioner is hereby authorized to charge any fees due under 37 C.F.R. §§1.16 or 1.17, or to credit any overpayments, to Deposit Account No. 50-4262 in order to have this information disclosure statement considered.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/John Nortrup/	Date (YYYY-MM-DD)	2011-12-05
Name/Print	John Nortrup	Registration Number	59,063

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	12/413,823
	Filing Date	Mar 30, 2009
	First Named Inventor	Robert J. Poston
	Art Unit	2431
	Examiner Name	TRAORE, Fatoumata
Sheet 3 of 3	Attorney Docket No.	SPHS-0031-P01

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Electronic Acknowledgement Receipt

EFS ID:	12546823
Application Number:	11428203
International Application Number:	
Confirmation Number:	3669
Title of Invention:	METHOD AND SYSTEM FOR CLASSIFICATION OF SOFTWARE USING CHARACTERISTICS AND COMBINATIONS OF SUCH CHARACTERISTICS
First Named Inventor/Applicant Name:	Ben Godwood
Customer Number:	43520
Filer:	Robert A. Mazzaresse/Paula Ng
Filer Authorized By:	Robert A. Mazzaresse
Attorney Docket Number:	SPHS-0007-P01
Receipt Date:	16-APR-2012
Filing Date:	30-JUN-2006
Time Stamp:	12:44:17
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	SPHS-0007-P01_041612_Form1449.pdf	80257 8c0fa6ee97f2f581b2d054686c5fa1d25d6c1083	no	3

Warnings:

Information:

This is not an USPTO supplied IDS fillable form					
2	Non Patent Literature	NPL-17_AutomatedDetectionOfRefactoringsInEvolvingComponents.pdf	207336	no	25
			a06533686aee5e94aedd34b2e904b597fb0e37af		
Warnings:					
Information:					
3	Non Patent Literature	NPL-18_SN12413823_NFOAR-031912.pdf	684022	no	19
			55c3fd74189600ad846455e01cc1ea01d889fcd9		
Warnings:					
Information:					
Total Files Size (in bytes):			971615		
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Godwood, et al.	Conf. No.: 3669
Application No.: 11/428,203	Examiner: Laforgia, C.
Filed: June 30, 2006	T.C./Art Unit: 2439
For: METHOD AND SYSTEM FOR CLASSIFICATION OF SOFTWARE USING CHARACTERISTICS AND COMBINATIONS OF SUCH CHARACTERISTICS	

AMENDMENT AND REPLY

Commissioner for Patents
PO Box 1450
Alexandria, Virginia 22313-1450

Examiner:

Please enter the following amendments and remarks, which are responsive to the
Office Action mailed on October 4, 2011.

A **Request for Extension of Time** appears on page 2 of this paper.

An **Amendment to the Claims** begins on page 3 of this paper.

Remarks/Arguments begin on page 7 of this paper.

Request for Extension of Time

The applicant requests a three month extension of time from January 4, 2012 until April 4, 2012 for responding to the outstanding action. The fee of \$1,270.00 specified by 37 C.F.R. § 1.17(a)(3) accompanies this request.

Amendments to the Claims

Please amend the claims according to the following claim listing, which replaces all prior versions and listings of the claims in this application:

1. (Currently Amended) A method for classifying software, said method comprising;
~~analyzing all functional elements of software;~~
providing a library of gene information including a number of classifications based on groupings of genes;
~~identifying at least one of a functional block and at least one property of said the software;~~
~~identifying one or more genes, wherein said gene is a single piece of functionality or a property of said software in said at least one of a functional block and a property each describing one or more of the at least one functional block and the at least one property of said the software as a sequence of APIs and strings;~~
~~matching said the one or more genes against one or more of the number of classifications defined by a groupings of genes using a processor;~~
~~classifying said the software based on said the matching to provide a classification for the software one or more classifications; and~~
~~notifying a user of said one or more classifications the classification of the software.~~
2. (Currently amended) The method of claim 1, wherein ~~said classifying step further comprises classifying said software as malware based on said one or more classifications~~ the classification for the software includes malware.
3. (Currently amended) The method of claim 1, wherein ~~said classifying step further comprises classifying said software as~~ the classification for the software includes unwanted software.
4. (Currently amended) The method of claim 1, further comprising unpacking ~~said the~~ the software.

5. (Currently amended) The method of claim 1, further comprising disassembling ~~said~~ the software.
6. (Currently amended) The method of claim 1, further comprising filtering ~~said~~ the software.
7. (Currently amended) The method of claim 1, further comprising unencrypting ~~said~~ the software.
8. (Currently amended) The method of claim 1, further comprising generating an output based on ~~said~~ the classifying of said software.
9. (Currently amended) The method of claim 1, further comprising disinfecting at least one of ~~said~~ the software and a computer containing the software when ~~said~~ the software is classified as malware.
10. (Currently amended) The method of claim 1, further comprising removing ~~said~~ the software when ~~said~~ the software is classified as malware or unwanted software.
11. (Currently amended) The method of claim 1, further comprising quarantining ~~said~~ the software when ~~said~~ the software is classified as malware or unwanted software.
12. (Currently amended) The method of claim 1, further comprising generating reports regarding ~~said~~ the software.
13. (Currently amended) The method of claims 1, further comprising blocking access to ~~said~~ the software when ~~said~~ the software is classified as malware or unwanted software.
14. (Currently amended) The method of claim 1, further comprising scanning a

computer for ~~said the~~ software, wherein ~~said the~~ scanning includes at least one of a user initiated scanning, a scheduled scanning and an on access scanning.

15. (Currently amended) The method of claim 1, wherein ~~said the~~ classification is based upon one or more groupings of genes.

16. (Currently Amended) A method for generating software classifications for use in classifying software, said method comprising:

~~analyzing all functional elements of software;~~

providing a library of gene information including a number of classifications based on groupings of genes;

~~identifying one or more genes, wherein a gene is a single piece of functionality or a property of software that appear in each describing a functionality or a property of said the software as a sequence of APIs and strings;~~

~~combining a plurality of genes that appear in describe the software, thereby providing a set of genes;~~

~~testing said the set of genes for false-positives against one or more reference files using a processor;~~

~~defining a the software classification based on said the set of genes; and~~

storing the set of genes and the software classification in the library.

~~returning a result of said software classification based on said set of genes to a user.~~

17. (Currently amended) The method of claim 16, wherein ~~said the~~ software classification ~~classifies~~ includes malware.

18. (Currently amended) The method of claim 16, wherein ~~said the~~ software classification ~~classifies~~ includes unwanted software.

19-33. (Canceled)

34. (New) The method of claim 16 further comprising returning a result of the software classification to a user.

35. (New) The method of claim 16 further comprising unpacking the software before identifying one or more genes.

36. (New) The method of claim 16 further comprising filtering the software before identifying one or more genes to determine whether the software requires further analysis.

Remarks

Claim Status

Claims 1-18 are amended. Claims 19-33 are canceled. New claims 34-36 are added. Claims 1-18 and 34-36 are presented for examination, with claims 1 and 16 being independent.

Claim Rejections – 35 USC § 103

The claims stand rejected under 35 U.S.C. § 103(a) as unpatentable over U.S. Pat. Pub. No. 2008/0040710 to Chiriac (“*Chiriac*”) in view of U. S. Pat. Pub. No. 2006/0123244 to Gheorghescu, et al. (“*Gheorghescu*”).

The applicant has devised a technique for identifying unwanted software using genes that characterize functional portions of software as sequences of APIs and strings. These ‘genes’ can be compared against a library of such genes to classify software according to specific or similarities in functionality without requiring line-by-line identity of code. The claims have been amended to clarify this inventive concept. The art of record does not specifically disclose genes, or any other technique similarly employing sequences of APIs and strings to describe software, or any use of groups of such genes to classify software.

Gheorghescu discloses techniques for “translating potential malware devices [sic] into safe program code.”¹ As a necessary prerequisite, the potential malware must be located. “Before and/or during execution, the present invention causes a scanner to search for potential malware . . .”² *Gheorghescu* generally proposes scanning on a “block” level based upon “sequences of program code that contain only a single entry point at the beginning of the sequence and a single exit point at the end of the sequence.”³ According to *Gheorghescu*, this approach permits dynamic remediation where a “selected instruction is translated into safe program code that is in an architecture-neutral format.”⁴

However, in terms of the *type(s)* of scanning contemplated by *Gheorghesu*, there

¹ *Gheorghescu*, Abstract.

² *Gheorghescu*, Abstract.

³ *Gheorghescu*, ¶ [0022].

⁴ *Gheorghescu*, ¶ [0043].

appears to be little if anything that expands upon known malware detection techniques, except for adaptations of these known techniques to *Gheorghescu*'s block-level scanning:

[T]he malware detection system 200 includes a scanner 204 designed to detect malware. As known to those skilled in the art and others, many different software vendors include a scanner in antivirus software that is configured to identify program code characteristic of malware. Unfortunately, existing scanners are not configured to work in conjunction with a system that translates potential malware into safe program code prior to execution. Instead, some existing scanners work in conjunction with the type of emulation system described above. In these systems, the scanner adds additional overhead so that the emulation process may take an unreasonable amount of time. However, the software routines implemented by the present invention provide the scanner 204 with the infrastructure needed to quickly identify obscured malware such as malware that is "unpacked" (i.e., decrypted) or otherwise loaded into memory at runtime.⁵

Thus *Gheorghescu* addresses a fundamentally different issue of malware detection – when the detection occurs (at each new “block” of code) and how it is remediated (by translating into safe code) – than the claimed invention, which focuses instead on *how* malware is detected. In this respect, the applicant has proposed characterizing functional aspects of code using sequences of APIs and strings, referred to as “genes,” that describe software. This notion is entirely absent from *Gheorghescu*.

Chiriac does not fill the void left by *Gheorghescu*. Instead *Chiriac* appears to focus on the challenges of detecting obfuscated viral code. To be sure, *Chiriac* suggests the importance of APIs in generalized malware detection. During decompression, “APIs (application program interfaces) are monitored” to detect API hijacking.⁶ However, *Chiriac* does not specifically suggest the use of genes or any similar software descriptions. Instead *Chiriac* proposes a staged sequence of techniques and flags during decompression and execution of code to optimize threat detection:

In summary, the file is first inspected for type and "obvious" or known indicators that it is malware. Then, the running of the file on the host computer is emulated in a safe, virtual environment created on the host computer so as to allow the file to be unpacked/decrypted and to collect execution-level flags. Then, the image of the decrypted file is analyzed in combination with the API (application program interface) data obtained

⁵ *Gheorghescu*, ¶ [0021].

⁶ *Chiriac*, ¶ [0053].

during the emulation to determine whether or not it is or should be classed as malware.⁷

Chiriac provides significantly more detail with respect to these various stages of processing; however, *Chiriac* does not suggest any use of the claimed ‘genes’ or any analogous functional description of software using sequences of APIs and strings as a basis for classifying software.

More specifically with respect to claim 1, none of the art of record teaches, suggests, or otherwise renders obvious a method that includes identifying one or more genes each describing one or more of the at least one functional block and the at least one property of the software as a sequence of APIs and strings; matching the one or more genes against a number of classifications using a processor; and classifying the software based on the matching to provide a classification for the software. For similar reasons, claim 16 is patentable over *Chiriac* and *Gheorghescu*. The remaining claims depend from an allowable base claim and are likewise believed to be in condition for allowance.

⁷ *Chiriac*, ¶

Conclusion

The claims currently pending in this case are believed to be in condition for allowance. The applicant therefore requests that the examiner withdraw any outstanding objections and rejections and issue a notice of allowance for same.

It is believed that all of the pending claims have been addressed. However, the absence of a reply to a specific rejection, issue, or comment does not signify agreement with or concession of that rejection, issue, or comment. In addition, the arguments made above may not be exhaustive. Thus, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this paper, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

The Commissioner is hereby authorized to charge any additional required fees to Deposit Account No. 50-4262 in order to have this amendment considered. The examiner is encouraged to contact the undersigned if there are any questions concerning this submission.

Respectfully submitted,
STRATEGIC PATENTS, P.C.

/ Robert A. Mazzaresse /
Robert A. Mazzaresse
Reg. No. 42,852
(781) 453-9993

April 3, 2012

Electronic Patent Application Fee Transmittal

Application Number:	11428203			
Filing Date:	30-Jun-2006			
Title of Invention:	METHOD AND SYSTEM FOR CLASSIFICATION OF SOFTWARE USING CHARACTERISTICS AND COMBINATIONS OF SUCH CHARACTERISTICS			
First Named Inventor/Applicant Name:	Ben Godwood			
Filer:	John H. Nortrop			
Attorney Docket Number:	SPHS-0007-P01			
Filed as Large Entity				
Utility under 35 USC 111(a) Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 3 months with \$0 paid	1253	1	1270	1270

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Total in USD (\$)				1270

Electronic Acknowledgement Receipt

EFS ID:	12457222
Application Number:	11428203
International Application Number:	
Confirmation Number:	3669
Title of Invention:	METHOD AND SYSTEM FOR CLASSIFICATION OF SOFTWARE USING CHARACTERISTICS AND COMBINATIONS OF SUCH CHARACTERISTICS
First Named Inventor/Applicant Name:	Ben Godwood
Customer Number:	43520
Filer:	John H. Nortrop
Filer Authorized By:	
Attorney Docket Number:	SPHS-0007-P01
Receipt Date:	03-APR-2012
Filing Date:	30-JUN-2006
Time Stamp:	14:15:24
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$ 1270
RAM confirmation Number	446
Deposit Account	504262
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		SPHS-0007-P01_040312_OAResponse.pdf	123743 1183e2d089588d71f064b38f5bf6540c6b8e ce9b	yes	10
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Amendment/Req. Reconsideration-After Non-Final Reject		1	1	
	Extension of Time		2	2	
	Claims		3	6	
	Applicant Arguments/Remarks Made in an Amendment		7	10	

Warnings:**Information:**

2	Fee Worksheet (SB06)	fee-info.pdf	30616 1524eb6755862e7358b0511b8f59e052281 586cc	no	2
---	----------------------	--------------	---	----	---

Warnings:**Information:**

Total Files Size (in bytes):	154359
-------------------------------------	--------

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875					Application or Docket Number 11/428,203		Filing Date 06/30/2006		<input type="checkbox"/> To be Mailed	
APPLICATION AS FILED – PART I										
(Column 1)			(Column 2)			SMALL ENTITY <input type="checkbox"/> OR		OTHER THAN SMALL ENTITY		
FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)	OR	RATE (\$)	FEE (\$)			
<input type="checkbox"/> BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A				
<input type="checkbox"/> SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A			N/A				
<input type="checkbox"/> EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A				
TOTAL CLAIMS (37 CFR 1.16(j))	minus 20 =	*	X \$	=		X \$	=			
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X \$	=		X \$	=			
<input type="checkbox"/> APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).									
<input type="checkbox"/> MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))										
* If the difference in column 1 is less than zero, enter "0" in column 2.										
APPLICATION AS AMENDED – PART II										
(Column 1)			(Column 2)			SMALL ENTITY OR		OTHER THAN SMALL ENTITY		
AMENDMENT	04/03/2012	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	OR	RATE (\$)	ADDITIONAL FEE (\$)
	Total (37 CFR 1.16(i))	* 21	Minus	** 33	= 0	X \$	=		X \$60=	0
	Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0	X \$	=		X \$250=	0
	<input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))									
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))									
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	0
(Column 1)			(Column 2)			SMALL ENTITY OR		OTHER THAN SMALL ENTITY		
AMENDMENT	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	OR	RATE (\$)	ADDITIONAL FEE (\$)	
	Total (37 CFR 1.16(i))	*	Minus	**	=	X \$	=	X \$	=	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X \$	=	X \$	=	
	<input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))									
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))									
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3. ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3". The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.										

Legal Instrument Examiner:
/RUTH LLOYD/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/428,203	06/30/2006	Ben Godwood	SPHS-0007-P01	3669

43520 7590 10/04/2011
STRATEGIC PATENTS P.C..
C/O CPA Global
P.O. BOX 52050
MINNEAPOLIS, MN 55402

EXAMINER

LAFORGIA, CHRISTIAN A

ART UNIT	PAPER NUMBER
----------	--------------

2439

NOTIFICATION DATE	DELIVERY MODE
-------------------	---------------

10/04/2011

ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@cpaglobal.com
Patents@strategic-patents.com

Office Action Summary	Application No.	Applicant(s)	
	11/428,203	GODWOOD ET AL.	
	Examiner	Art Unit	
	Christian LaForgia	2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 09 June 2011.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on ____; the restriction requirement and election have been incorporated into this action.
- 4) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 5) ☒ Claim(s) 1-33 is/are pending in the application.
- 5a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 6) ☐ Claim(s) ____ is/are allowed.
- 7) ☒ Claim(s) 1-33 is/are rejected.
- 8) ☐ Claim(s) ____ is/are objected to.
- 9) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 10) ☐ The specification is objected to by the Examiner.
- 11) ☒ The drawing(s) filed on 30 June 2006 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 12) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. ____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. ____. |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date ____. | 6) <input type="checkbox"/> Other: ____. |

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 09 June 2011 has been entered.
2. Claims 1-33 have been presented for examination.

Response to Arguments

3. Applicant's arguments, see page 7, filed 09 June 2011, with respect to the rejections made under 35 U.S.C. § 101 have been fully considered and are persuasive. The 35 U.S.C. § 101 rejection of claims 19-33 has been withdrawn.
4. Applicant's arguments with respect to prior art rejection of claims 1-33 have been considered but are moot in view of the new grounds of rejection set forth below.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 1-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application Publication No. 2008/0040710 A1 to Chiriac, hereinafter Chiriac, in view of U.S.

Art Unit: 2439

Patent Application Publication No. 2006/0123244 A1 to Gheorghescu et al., hereinafter Gheorghescu.

7. As per claims 1 and 19, Chiriac teaches method and a non-transitory computer-readable medium comprising instructions for classifying software, said method comprising:

analyzing all functional elements of software (paragraphs 0039, 0048, 0056, scanning the file in three main states to determine whether it should be treated as malware);

identifying at least one of a functional block and a property of said software (paragraphs 0010, 0030, 0032, 0066, partitioning the executable computer file into plural basic blocks of code);

identifying one or more genes, wherein said gene is a single piece of functionality or property of said software in said at least one of a functional block and a property of said software (paragraph 0030, 0032, 0048-0054, executing the basic blocks to determine the execution-level flags (properties) associated with the basic block);

matching said one or more genes against one or more classifications defined by a groupings of genes using a processor (paragraphs 0030, 0032, 0055, 0066-0068, using any execution-level flags to aid in malware analysis of the file); and

classifying said software based on said one or more classifications (paragraphs 0030, 0032, 0056, determining whether the executable should be classed as malware).

8. Chiriac does not teach notifying a user of said one or more classifications.

9. Gheorghescu teaches notifying a user of said one or more classifications (Figure 4 [step 420], paragraphs 0038, 0039).

Art Unit: 2439

10. It would have been obvious to one of ordinary skill in the art at the time the invention was made to notify a user of the classification of the software, since one of ordinary skill in the art would recognize that notifying the user would allow them to take remedial action if the software was identified as malware or execute the code if it was identified as non-malware.

11. Regarding claims 2 and 20, Chiriac teaches wherein said classifying step further comprises classifying said software as malware based on said one or more classifications (paragraphs 0030, 0032, 0056, determining whether the executable should be classed as malware based on the execution-level flags raised).

12. Regarding claims 3 and 21, Chiriac teaches wherein said classifying step further comprises classifying said software as unwanted software (paragraphs 0030, 0032, 0056, determining whether the executable should be classed as malware).

13. Regarding claims 4 and 22, Chiriac teaches unpacking said software (Abstract, paragraphs 0010, 0013).

14. Regarding claims 5 and 23, Chiriac teaches disassembling said software (Figure 1 [item 34], paragraphs 0065, 00698).

15. Regarding claims 6 and 24, Chiriac teaches filtering said software (Figure 1 [item 36], paragraphs 0012-0014, 0069, 0070).

16. Regarding claims 7 and 25, Chiriac teaches unencrypting said software (Abstract, paragraphs 0010, 0013).

17. Regarding claims 8 and 26, Chiriac teaches generating an output based on said classifying of said software (paragraphs 0030, 0032, 0056, determining whether the executable should be classed as malware).

18. Regarding claims 9 and 27, Gheorghescu teaches disinfecting at least one of said software and a computer when said software is classified as malware (paragraphs 0042, 0043, i.e. translating the program into safe program code).

19. Regarding claims 10 and 28, Gheorghescu teaches removing said software when said software is classified as malware or unwanted software (paragraphs 0042, 0043, i.e. translating the program into safe program code).

20. Regarding claims 11 and 29, Gheorghescu teaches quarantining said software when said software is classified as malware or unwanted software (paragraph 0004).

21. Regarding claims 12 and 30, Gheorghescu teaches generating reports regarding said software (Figure 4 [step 420], paragraphs 0038, 0039).

Art Unit: 2439

22. Regarding claims 13 and 31, Gheorghescu teaches blocking access to said software when said software is classified as malware or unwanted software (paragraphs 0042, 0043).

23. Regarding claims 14 and 32, Gheorghescu teaches scanning a computer for said software, wherein said scanning include user initiated scanning, scheduled scanning and on-access scanning (Figure 4 [step 416], paragraphs 0038, 0040).

24. Regarding claim 15, Chiriac teaches wherein said classification is based upon one or more groupings of genes (paragraphs 0030, 0032, 0056, determining whether the executable should be classed as malware).

25. As per claim 16, Chiriac teaches a method for generating software classifications for use in classifying software, said method comprising:

analyzing all functional elements of software (paragraphs 0039, 0048, 0056, scanning the file in three main states to determine whether it should be treated as malware);

identifying one or more genes that appear in software, wherein a gene is a single piece of functionality or a property of software that appear in said software (paragraph 0030, 0032, 0048-0054, executing the basic blocks to determine the execution-level flags (properties) associated with the basic block);

combining a plurality of genes to form a set of genes (paragraphs 0030, 0032, 0056, determining whether the executable should be classed as malware based on a plurality of execution level flags);

Art Unit: 2439

testing said set of genes for false-positives against one or more reference files using a processor (paragraphs 0030, 0032, 0055, 0066-0068, using any execution-level flags to aid in malware analysis of the file); and

defining a software classification based on said set of genes (paragraphs 0030, 0032, 0056, determining whether the executable should be classed as malware).

26. Chiriac does not teach returning a result of said software classification based on said set of genes to a user.

27. Gheorghescu teaches returning a result of said software classification based on said set of genes to a user (Figure 4 [step 420], paragraphs 0038, 0039).

28. It would have been obvious to one of ordinary skill in the art at the time the invention was made to make a user aware of the software classification, since one of ordinary skill in the art would recognize that notifying the user would allow them to take remedial action if the software was identified as malware or execute the code if it was identified as non-malware.

29. Regarding claim 17, Chiriac teaches wherein said software classification classifies malware (paragraphs 0030, 0032, 0056, determining whether the executable should be classed as malware).

30. Regarding claim 18, Chiriac teaches wherein said software classification classifies unwanted software (paragraphs 0030, 0032, 0056, determining whether the executable should be classed as malware).

Art Unit: 2439

31. Regarding claim 33, Chiriac teaches a classification generation routine configured to generate software classifications, said classification routine executing the steps of:

identifying a software functionality (paragraph 0030, 0032, 0048-0054, executing the basic blocks to determine the execution-level flags (properties) associated with the basic block);

defining a characteristic based on said identified software functionality (paragraph 0030, 0032, 0048-0054, execution-level flags (properties) associated with the basic block); and

combining a plurality of characteristics to form a classification (paragraphs 0030, 0032, 0056, determining whether the executable should be classed as malware based on one or more of the execution level flags generated).

Conclusion

32. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

33. The following patents are cited to further show the state of the art, such as:

United States Patent Application Publication No. 2007/0016953 A1 to Morris et al., which is cited to show scanning the genes of a basic blocks to determine whether a program constitutes malware (paragraphs 0128, 0137).

United States Patent Application Publication No. 2009/0187992 A1 to Poston, which is cited to put a continuation in part of the instant application in the record.

United States Patent No. 6,301,699 B1 to Hollander et al., which is cited to show detecting a buffer overflow attack by analyzing the basic blocks of a program.

Art Unit: 2439

34. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian LaForgia whose telephone number is (571)272-3792.

The examiner can normally be reached on Monday thru Thursday 7-5.

35. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad can be reached on (571) 272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

36. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christian LaForgia/
Primary Examiner, Art Unit 2439

clf

Notice of References Cited	Application/Control No. 11/428,203	Applicant(s)/Patent Under Reexamination GODWOOD ET AL.	
	Examiner Christian LaForgia	Art Unit 2439	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-6,301,699 B1	10-2001	Hollander et al.	717/131
*	B	US-2007/0016953 A1	01-2007	Morris et al.	726/024
*	C	US-2008/0040710 A1	02-2008	CHIRIAC, MIHAI	717/136
*	D	US-2009/0187992 A1	07-2009	Poston, Robert J.	726/24
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			


FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

<i>Index of Claims</i> 	Application/Control No. 11428203	Applicant(s)/Patent Under Reexamination GODWOOD ET AL.
	Examiner Christian LaForgia	Art Unit 2439

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

<input type="checkbox"/> Claims renumbered in the same order as presented by applicant		<input type="checkbox"/> CPA		<input type="checkbox"/> T.D.		<input type="checkbox"/> R.1.47			
CLAIM		DATE							
Final	Original	05/14/2010	03/07/2011	09/28/2011					
	1	✓	✓	✓					
	2	✓	✓	✓					
	3	✓	✓	✓					
	4	✓	✓	✓					
	5	✓	✓	✓					
	6	✓	✓	✓					
	7	✓	✓	✓					
	8	✓	✓	✓					
	9	✓	✓	✓					
	10	✓	✓	✓					
	11	✓	✓	✓					
	12	✓	✓	✓					
	13	✓	✓	✓					
	14	✓	✓	✓					
	15	✓	✓	✓					
	16	✓	✓	✓					
	17	✓	✓	✓					
	18	✓	✓	✓					
	19	✓	✓	✓					
	20	✓	✓	✓					
	21	✓	✓	✓					
	22	✓	✓	✓					
	23	✓	✓	✓					
	24	✓	✓	✓					
	25	✓	✓	✓					
	26	✓	✓	✓					
	27	✓	✓	✓					
	28	✓	✓	✓					
	29	✓	✓	✓					
	30	✓	✓	✓					
	31	✓	✓	✓					
	32	✓	✓	✓					
	33	✓	✓	✓					

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	3	sophos.as.	US-PGPUB; USPAT	OR	ON	2010/05/13 09:11
S2	3	godwood-ben\$.in.	US-PGPUB; USPAT	OR	ON	2010/05/13 09:11
S3	4	mccourt-william\$.in.	US-PGPUB; USPAT	OR	ON	2010/05/13 09:14
S4	2	("20050172338" "20040181677").pn.	US-PGPUB; USPAT	OR	ON	2010/05/13 09:16
S5	5	("2005/0172338").URPN.	USPAT	OR	OFF	2010/05/13 09:21
S6	0	("2004/0181677").URPN.	USPAT	OR	OFF	2010/05/13 09:22
S7	0	("2004/0181677").URPN.	USPAT	OR	OFF	2010/05/13 09:22
S8	1	(anti\$virus (malware virus trojan adware spyware dialer) near detect\$3) same (detect\$3 determin \$5) with (malware malicious trojan adware spyware dialer) with (decompil\$3 disassembl \$3) with (program code)	US-PGPUB; USPAT	OR	ON	2010/05/13 09:25
S9	8	(detect\$3 determin\$5) with (malware malicious trojan adware spyware dialer) with (decompil\$3 disassembl\$3) with (program code)	US-PGPUB; USPAT	OR	ON	2010/05/13 09:27
S10	63	(detect\$3 determin\$5) with (malware malicious trojan adware spyware dialer) with (characteristic) with (program code)	US-PGPUB; USPAT	OR	ON	2010/05/13 09:30
S11	8	(detect\$3 determin\$5) with (malware malicious trojan adware spyware dialer) with (characteristic) with (program code) and (disassembl\$3 unpack\$3)	US-PGPUB; USPAT	OR	ON	2010/05/13 09:31

S13	3	("2006/0123244").URPN.	USPAT	OR	OFF	2010/05/13 11:20
S14	11	((("20050005153") or ("20040041315") or ("5381533") or ("5765030") or ("20020091934") or ("6704925") or ("5826013") or ("5951698") or ("6357008") or ("20030101381") or ("6637514")).PN.	US-PGPUB; USPAT	OR	OFF	2010/05/13 11:28
S15	77	("6357008").URPN.	USPAT	OR	OFF	2010/05/13 11:30
S16	74	("5826013").URPN.	USPAT	OR	OFF	2010/05/13 11:38
S17	1	(US-20060123244-\$).did.	US-PGPUB	OR	OFF	2010/05/13 12:22
S18	1	S17 and quarantin\$3	US-PGPUB; USPAT	OR	ON	2010/05/13 12:22
S19	18	726/24.ccls. and program with API near call	US-PGPUB; USPAT	OR	OFF	2011/03/07 11:49
S20	29	(scan\$4 check\$3 determin \$5 detect\$3) with API near call with (malware malicious virus trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2011/03/07 11:52
S21	3	("20040181677" "20050172338" "20090187992").pn.	US-PGPUB; USPAT	OR	OFF	2011/03/07 12:04
S22	13	726/24.ccls. and gene	US-PGPUB; USPAT	OR	ON	2011/03/07 12:06
S23	1	(US-20060123244-\$).did.	US-PGPUB	OR	OFF	2011/03/07 12:56
S24	1	S23 and basic adj block	US-PGPUB; USPAT	OR	ON	2011/03/07 12:56
S25	5387	726/22-24.ccls.	US-PGPUB; USPAT	OR	OFF	2011/09/27 14:05
S26	5	726/22-24.ccls. and basic near block with (property function\$6)	US-PGPUB; USPAT	OR	ON	2011/09/27 14:06
S27	0	(monitor\$3 scan\$4) with basic near block with (property function\$6) with (detect\$3 determin\$5 check\$3) near3 (malware malicious virus trojan spy \$ware ad\$ware)	US-PGPUB; USPAT	OR	ON	2011/09/27 14:08

S28	2	(monitor\$3 scan\$4) with basic near block with (property function\$6) same (detect\$3 determin\$5 check\$3) near3 (malware malicious virus trojan spy\$ware ad\$ware)	US-PGPUB; USPAT	OR	ON	2011/09/27 14:08
S29	0	basic near block with (property function\$6) with (detect\$3 determin\$5 check\$3) near3 (malware malicious virus trojan spy \$ware ad\$ware)	US-PGPUB; USPAT	OR	ON	2011/09/27 14:11
S30	2	basic near block with (property function\$6) same (detect\$3 determin\$5 check\$3) near3 (malware malicious virus trojan spy\$ware ad\$ware)	US-PGPUB; USPAT	OR	ON	2011/09/27 14:13
S31	2	basic near block with (property function\$6) same (detect\$3 determin\$5 check\$3) near3 (malware malicious virus trojan spy\$ware ad\$ware)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/09/27 14:13
S32	156	S25 and "717".clas.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/09/27 14:14
S33	7	S25 and "717".clas. and basic near block	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/09/27 14:14
S34	0	(monitor\$3 scan\$4) with basic near block with heuristic\$4	US-PGPUB; USPAT	OR	ON	2011/09/27 14:30
S35	1	(monitor\$3 scan\$4) with (basic code) near2 block with heuristic\$4	US-PGPUB; USPAT	OR	ON	2011/09/27 14:30
S36	21	(monitor\$3 scan\$4 detect \$3 determin\$5) with (basic code) near2 block with heuristic\$4	US-PGPUB; USPAT	OR	ON	2011/09/27 14:31
S37	1	(monitor\$3 scan\$4 detect \$3 determin\$5) with (basic code) near2 block with heuristic\$4 and "726". clas.	US-PGPUB; USPAT	OR	ON	2011/09/27 14:31


S38	5387	726/22-24.ccls.	US-PGPUB; USPAT	OR	OFF	2011/09/27 14:32
S39	5387	S38	US-PGPUB; USPAT	OR	ON	2011/09/27 14:32
S40	48	S39 and gene	US-PGPUB; USPAT	OR	ON	2011/09/27 14:32
S41	1	"20080040710".pn.	US-PGPUB; USPAT	OR	ON	2011/09/27 14:38
S42	0	S39 and gene	EPO	OR	ON	2011/09/27 14:41
S43	2	("2008/0040710").URPN.	USPAT	OR	OFF	2011/09/27 14:42
S44	0	("7996904").URPN.	USPAT	OR	OFF	2011/09/27 14:42
S45	1	"20080040710".pn.	US-PGPUB; USPAT	OR	ON	2011/09/27 16:25
S46	0	S45 and notif\$7	US-PGPUB; USPAT	OR	ON	2011/09/27 16:25
S47	0	S45 and alert\$3	US-PGPUB; USPAT	OR	ON	2011/09/27 16:25
S48	1	S45 and unpack\$3	US-PGPUB; USPAT	OR	OFF	2011/09/27 16:30
S49	0	S45 and filter\$3	US-PGPUB; USPAT	OR	OFF	2011/09/27 16:31
S50	1	S45 and translat\$3	US-PGPUB; USPAT	OR	OFF	2011/09/27 16:32
S51	0	S45 and unencrypt\$3	US-PGPUB; USPAT	OR	OFF	2011/09/27 16:33
S52	1	S45 and decrypt\$3	US-PGPUB; USPAT	OR	OFF	2011/09/27 16:33

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S12	1	sophos.as.	USPAT; UPAD	OR	ON	2010/05/13 09:11

9/ 28/ 11 9:02:43 AM

C:\Documents and Settings\claforgia\My Documents\EAST\Workspaces\11428203.wsp

Search Notes 	Application/Control No. 11428203	Applicant(s)/Patent Under Reexamination GODWOOD ET AL.
	Examiner Christian LaForgia	Art Unit 2439

SEARCHED			
Class	Subclass	Date	Examiner
none	none	5/13/10	clf
726	24	3/7/11	clf
726	22-24	9/27/11	clf

SEARCH NOTES		
Search Notes	Date	Examiner
EAST search - see enclosed	5/13/10	clf
IEEE search	5/13/10	clf
ACM search	5/13/10	clf
Google search	5/13/10	clf
Inventor search	5/13/10	clf
Assignee search	5/13/10	clf
updated EAST - see enclosed	3/7/11	clf
updated EAST - see enclosed	9/27/11	clf

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

	/Christian LaForgia/ Primary Examiner.Art Unit 2439
--	--

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Godwood, et al.	Conf. No.: 3669
Application No.: 11/428,203	Examiner: Laforgia, C.
Filed: June 30, 2006	T.C./Art Unit: 2439
For: METHOD AND SYSTEM FOR CLASSIFICATION OF SOFTWARE USING CHARACTERISTICS AND COMBINATIONS OF SUCH CHARACTERISTICS	

REQUEST FOR CONTINUED EXAMINATION

Commissioner for Patents
PO Box 1450
Alexandria, Virginia 22313-1450

Examiner:

In response to the Office Action mailed on March 16, 2011, the applicant requests continued examination of this application pursuant to 37 CFR 1.114. The fee of \$810 specified by 37 CFR 1.17(e) accompanies this request.

Please enter the following prior to continued examination:

An **Amendment to the Claims** begins on page 2 of this paper.

Remarks/Arguments begin on page 7 of this paper.

Amendments to the Claims

1. (Currently Amended) A method for classifying software, said method comprising;
analyzing all functional elements of software;
identifying at least one of a functional block and a property of said software;
identifying one or more genes, wherein said gene is a single piece of
functionality or a property of said software in said at least one of a functional block and
a property of said software;
matching said one or more genes against one or more classifications defined by
a groupings of genes using a processor;
classifying said software based on said one or more classifications; and
notifying a user of said one or more classifications.
2. (Original) The method of claim 1, wherein said classifying step further comprises
classifying said software as malware based on said one or more classifications.
3. (Original) The method of claim 1, wherein said classifying step further comprises
classifying said software as unwanted software.
4. (Original) The method of claim 1, further comprising unpacking said software.
5. (Original) The method of claim 1, further comprising disassembling said software.
6. (Original) The method of claim 1, further comprising filtering said software.
7. (Original) The method of claim 1, further comprising unencrypting said software.
8. (Original) The method of claim 1, further comprising generating an output based on
said classifying of said software.
9. (Original) The method of claim 1, further comprising disinfecting at least one of said

software and a computer when said software is classified as malware.

10. (Original) The method of claim 1, further comprising removing said software when said software is classified as malware or unwanted software.

11. (Original) The method of claim 1, further comprising quarantining said software when said software is classified as malware or unwanted software.

12. (Original) The method of claim 1, further comprising generating reports regarding said software.

13. (Original) The method of claims 1, further comprising blocking access to said software when said software is classified as malware or unwanted software.

14. (Original) The method of claim 1, further comprising scanning a computer for said software, wherein said scanning include user initiated scanning, scheduled scanning and on access scanning.

15. (Original) The method of claim 1, wherein said classification is based upon one or more groupings of genes.

16. (Currently Amended) A method for generating software classifications for use in classifying software, said method comprising:

analyzing all functional elements of software;

identifying one or more genes, wherein a gene is a single piece of functionality or a property of software that appear in said software;

combining a plurality of genes that appear in software;

testing said set of genes for false-positives against one or more reference files using a processor;

defining a software classification based on said set of genes; and

returning a result of said software classification based on said set of genes to a user.

17. (Original) The method of claim 16, wherein said software classification classifies malware.

18. (Original) The method of claim 16, wherein said software classification classifies unwanted software.

19. (Currently Amended) A non-transitory computer-readable medium having a set of instructions for execution on a computer, said set of instructions comprising:

an analysis routine configured to analyze all functional elements of software;

an identification routine configured to identify one or more functional blocks and/or properties of software;

a routine configured to identify genes in said one or more functional blocks and/or properties, wherein said gene is a piece of functionality or property of said software;

a matching routine configured to match genes against a list of predetermined classifications defined by groupings of genes using a processor;

a classification routine configured to classify said software; and

a reporting routine configured to report said classifying of said software.

20. (Original) The set of instructions of claim 19, wherein said classification routine is configured to classify malware.

21. (Original) The set of instructions of claim 19, wherein said classification routine is configured to classify unwanted software.

22. (Original) The set of instructions of claim 19, further comprising an unpacking routine configured to unpack said software.

23. (Original) The set of instructions of claim 19, further comprising a disassembly routine configured to disassemble said software.

24. (Original) The set of instructions of claim 19, further comprising a filtering routine configured to filter said software

25. (Original) The set of instructions of claim 19, further comprising an unencryption routine configured to unencrypt said software.

26. (Original) The set of instructions of claim 19, further comprising an output routine configured to generate an output based on a classification of said software.

27. (Original) The set of instructions of claim 19, further comprising a disinfection routine configured to disinfect said software when said software is classified as malware.

28. (Original) The set of instructions of claim 19, further comprising a removal routine configured to removed said software when said software is classified as malware or unwanted software.

29. (Original) The set of instructions of claim 19, further comprising a quarantine routine configured to quarantine of said software when said software is classified as malware or unwanted software.

30. (Original) The set of instructions of claim 19, further comprising a reporting routine configured to generate reports regarding said software.

31. (Original) The set of instructions of claim 19, further comprising a blocking routine configured to block access to said software when said software is classified as malware or unwanted software.

32. (Original) The set of instructions of claim 19, further comprising a scanning routine configured to scan a computer for said software, said scanning including at least one of user initiated scanning, scheduled scanning and on-access scanning.

33. (Original) The set of instructions of claim 19, further comprising a classification generation routine configured to generate software classifications, said classification routine executing the steps of:

- identifying a software functionality;
- defining a characteristic based on said identified software functionality; and
- combining a plurality of characteristics to form a classification.

Remarks

Claim Status

Claims 1, 16, and 19 are amended. Claims 1-33 are presented for examination, with claims 1, 16, and 19 being independent.

Claim Rejections – 35 U.S.C. § 101

Claims 19-33 stand rejected under 35 USC § 101 as being directed to non-statutory subject matter. These claims have been amended so that they are directed to a non-transitory computer readable medium. The applicant requests reconsideration and withdrawal of the claim rejections under 35 U.S.C. § 101.

Claim Rejections – 35 USC § 102

The claims stand rejected under 35 U.S.C. § 102 as anticipated by U. S. Pat. Pub. No. 2006/0123244 to Gheorghescu, et al. (“Gheorghescu”).

Claim 1 includes the limitation of “analyzing all functional elements of software”. This limitation is not disclosed by the Gheorghescu reference for the reasons given below.

Gheorghescu discloses translating blocks of program code that have been scanned and found to contain malware, into code that can be safely executed. The level of scrutiny is limited to the basic block, and individual elements of functionality are not directly analyzed. The program is broken into “basic blocks” and the blocks are then scanned for malware, and if necessary, translated. In making the rejection the examiner states that Gheorghescu describes a basic block as follows: “basic blocks are sequences of program code that contain only a single entry point at the beginning of the sequence and a single exit point at the end of the sequence”. (Paragraph [0022]). This basic block may contain still contain multiple genes, as defined in the specification. A gene is a single piece of the functionality or property of the software program.”

This is in contrast to the present invention where a gene is a single piece of functionality or a property of the program. The genes are matched against functional blocks of code and the functionality is determined by matching sequences of API calls

and the strings that are referenced. This matching is not done in Gheorghescu, where the goal of the operation is to translate potentially harmful code into code that may be safely executed.

The present invention looks at all functional elements of the program as part of the process of identifying malware and non-malware functionality. In the present invention a functional block is not limited to a single block as defined by Gheorghescu, and in fact, is most likely to include the whole of the executable portions of the file. (In other words, all functions.) A functional element in the present invention may mean unpacked code, or a “new” functional block created when a packed portion of code is unpacked by the unpackers. The new functional block is then scanned for genes. Thus, genes are not blocks as Gheorghescu defines blocks. Gheorghescu limits the translation to the basic blocks that were found to be likely to contain malware as a result of the scan. This is different from the present invention where all program functionality is examined. As such, claim 1 includes features that are not disclosed within the cited prior art reference.

Independent claim 19 includes the same limitation, and is allowable for the reasons provided above.

Independent claim 16 has been amended to bring it into conformity with the remaining independent claims with respect to the limitation discussed above, and is likewise believed to be in condition for allowance. In addition, the claimed genes function differently than the basic blocks found in Gheorghescu. As noted above with respect to claim 1, genes are not blocks as Gheorghescu defines blocks. The Examiner cites paragraph 0034 as disclosing, “combining a plurality of genes to form a set of genes”. The applicant disagrees. Paragraph 0034 discloses the idea of identifying successor basic blocks. This merely identifies the order of performing tasks within the program. In contrast, genes are a smaller piece of the functionality of the program and direct the processor to perform certain tasks or operations. Genes may be independent of the successive order in which operations are performed, and may cross multiple functional blocks of executable code. Furthermore, Gheorghescu is silent regarding “testing said set of genes for false-positives against one or more reference files” as further claimed in claim 16. Gheorghescu merely scans the program for malware.

Scanning is not the same as testing the code. The present invention examines functionality, not heuristics, as is the case with Gheorghescu.

The remaining claims depend from an allowable base claim, and are likewise believed to be in condition for allowance.

Conclusion

The claims currently pending in this case are believed to be in condition for allowance. The applicant therefore requests that the examiner withdraw any outstanding objections and rejections and issue a notice of allowance for same.

It is believed that all of the pending claims have been addressed. However, the absence of a reply to a specific rejection, issue, or comment does not signify agreement with or concession of that rejection, issue, or comment. In addition, the arguments made above may not be exhaustive. Thus, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this paper, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

The Commissioner is hereby authorized to charge any additional required fees to Deposit Account No. 50-4262 in order to have this amendment considered. The examiner is encouraged to contact the undersigned if there are any questions concerning this submission.

Respectfully submitted,
STRATEGIC PATENTS, P.C.

/ Robert A. Mazzaresse /
Robert A. Mazzaresse
Reg. No. 42,852
(781) 453-9993

June 8, 2011

Electronic Patent Application Fee Transmittal

Application Number:	11428203			
Filing Date:	30-Jun-2006			
Title of Invention:	METHOD AND SYSTEM FOR CLASSIFICATION OF SOFTWARE USING CHARACTERISTICS AND COMBINATIONS OF SUCH CHARACTERISTICS			
First Named Inventor/Applicant Name:	Ben Godwood			
Filer:	John H. Nortrop			
Attorney Docket Number:	SPHS-0007-P01			
Filed as Large Entity				
Utility under 35 USC 111(a) Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Request for continued examination	1801	1	810	810
Total in USD (\$)				810

Electronic Acknowledgement Receipt

EFS ID:	10265789
Application Number:	11428203
International Application Number:	
Confirmation Number:	3669
Title of Invention:	METHOD AND SYSTEM FOR CLASSIFICATION OF SOFTWARE USING CHARACTERISTICS AND COMBINATIONS OF SUCH CHARACTERISTICS
First Named Inventor/Applicant Name:	Ben Godwood
Customer Number:	43520
Filer:	John H. Nortrop
Filer Authorized By:	
Attorney Docket Number:	SPHS-0007-P01
Receipt Date:	09-JUN-2011
Filing Date:	30-JUN-2006
Time Stamp:	10:24:26
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$810
RAM confirmation Number	10095
Deposit Account	504262
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		SPHS-0007-P01_060911_RCE.pdf	124781 c02c99e0576e7bc4f77c164e280361dd25d829a8	yes	10
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Request for Continued Examination (RCE)		1	1	
	Claims		2	6	
	Applicant Arguments/Remarks Made in an Amendment		7	10	
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30679 e10810e9113c53b444692832d48ebac72b402cac	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			155460		
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p>New Applications Under 35 U.S.C. 111 If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p>National Stage of an International Application under 35 U.S.C. 371 If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p>New International Application Filed with the USPTO as a Receiving Office If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875					Application or Docket Number 11/428,203		Filing Date 06/30/2006		<input type="checkbox"/> To be Mailed	
APPLICATION AS FILED – PART I										
(Column 1)			(Column 2)			SMALL ENTITY <input type="checkbox"/> OR		OTHER THAN SMALL ENTITY		
FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)	OR	RATE (\$)	FEE (\$)			
<input type="checkbox"/> BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A				
<input type="checkbox"/> SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A			N/A				
<input type="checkbox"/> EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A				
TOTAL CLAIMS (37 CFR 1.16(j))	minus 20 =	*	X \$	=	OR	X \$	=			
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X \$	=		X \$	=			
<input type="checkbox"/> APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).									
<input type="checkbox"/> MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))										
			TOTAL			TOTAL				
APPLICATION AS AMENDED – PART II										
(Column 1)			(Column 2)			SMALL ENTITY OR		OTHER THAN SMALL ENTITY		
AMENDMENT	06/09/2011	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	OR	RATE (\$)	ADDITIONAL FEE (\$)	
	Total (37 CFR 1.16(i))	* 33	Minus	** 33	=	0	OR	X \$52=	0	
	Independent (37 CFR 1.16(h))	* 3	Minus	***3	=	0	OR	X \$220=	0	
<input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))										
<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR			
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	0	
(Column 1)			(Column 2)			SMALL ENTITY OR		OTHER THAN SMALL ENTITY		
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	OR	RATE (\$)	ADDITIONAL FEE (\$)	
	Total (37 CFR 1.16(i))	*	Minus	**	=		OR	X \$	=	
	Independent (37 CFR 1.16(h))	*	Minus	***	=		OR	X \$	=	
<input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))										
<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR			
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE		
<p>* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.</p> <p>** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".</p> <p>*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".</p> <p>The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.</p>										

Legal Instrument Examiner:
/BRENDA WEBB/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/428,203	06/30/2006	Ben Godwood	SPHS-0007-P01	3669

43520 7590 03/16/2011
STRATEGIC PATENTS P.C..
C/O CPA Global
P.O. BOX 52050
MINNEAPOLIS, MN 55402

EXAMINER

LAFORGIA, CHRISTIAN A

ART UNIT	PAPER NUMBER
----------	--------------

2439

NOTIFICATION DATE	DELIVERY MODE
-------------------	---------------

03/16/2011

ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@cpaglobal.com
Patents@strategic-patents.com

Office Action Summary	Application No. 11/428,203	Applicant(s) GODWOOD ET AL.	
	Examiner Christian LaForgia	Art Unit 2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 24 January 2011.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-33 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-33 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 30 June 2006 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date <u>12/20/10</u> | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. The amendment of 24 January 2011 has been noted and made of record.
2. Claims 1-33 have been presented for examination.

Response to Arguments

3. Applicant's arguments, see page 9, filed 24 January 2011, with respect to the objection to the specification have been fully considered and are persuasive. The objection of the specification has been withdrawn.

4. Applicant's arguments, see pages 9 and 10, filed 24 January 2011, with respect to the rejection of claims 1-18 under 35 U.S.C. § 101 have been fully considered and are persuasive. The 35 U.S.C. § 101 rejection of claims 1-18 has been withdrawn.

5. Applicant's arguments with respect to the 35 U.S.C. § 101 rejection of claims 19-33 filed 24 January 2011 have been fully considered but they are not persuasive. The Applicant has amended the specification and claim, and argues that this is enough to overcome the rejection. The Examiner disagrees. The specification still describes the invention in such a way that one of ordinary skill in the art could reasonably construe the claimed computer-readable medium to encompass transitory media. A transitory, propagating signal does not fall within any one of the four categories of patentable subject matter set forth in 35 U.S.C. § 101, and such claims are therefore ineligible for patent protection. In *re Nuijten*, 500 F.3d 1346, 1357 (Fed. Cir. 2007), *reh'g en banc denied*, 515 F.3d 1361 (Fed. Cir. 2008), cert. denied, 129 S.Ct. 70 (2008). The PTO's preferred claim language is a "non-transitory computer-readable medium." The Applicant is encouraged to adopt this language to obviate this rejection.

Art Unit: 2439

6. Applicant's arguments with respect to the prior art rejections filed 24 January 2011 have been fully considered but they are not persuasive.

7. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies, specifically that a gene is a piece of functionality or a property of the program, are not recited in the rejected claims. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

8. The Examiner also sets forth that a basic block is a piece of functionality or a property of the program. As Gheorghescu sets forth in paragraph 0022, "basic blocks are sequences of program code that contain only a single entry point at the beginning of the sequence and a single exit point at the end of the sequence." At the very least, Gheorghescu's definition of a basic block satisfies the Applicant's assertion that a gene is a piece of functionality of a program.

9. Furthermore, the Applicant's specification describes functional blocks (see, e.g. paragraph 19), which the Examiner has interpreted to be on par with the disclosed basic blocks. The genes in the basic blocks are the lines and sequences of code that are compared to virus signatures. Therefore, Gheorghescu teaches the claimed limitations, and the rejection is maintained.

10. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies, specifically that the present invention looks at all functional elements of the program, are not recited in the rejected claims. Although the claims are interpreted in light of the specification, limitations from

Art Unit: 2439

the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

11. See further rejections set forth below.

Information Disclosure Statement

12. The information disclosure statement (IDS) submitted on 20 December 2010 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Claim Rejections - 35 USC § 101

13. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

14. Claims 19-33 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Paragraph 29 bridging pages 8 and 9 of the Specification of the instant application describes that the present invention can be implemented in a distributed network where different processes occur on different machines with a communication network to allow sharing of information. One of ordinary skill in the art could reasonably interpret this as defining computer-readable medium to include communication networks, which entail transitory signals. A transitory, propagating signal does not fall within any one of the four categories of patentable subject matter set forth in 35 U.S.C. § 101, and such claims are therefore ineligible for patent protection. In *re Nuijten*, 500 F.3d 1346, 1357 (Fed. Cir. 2007), *reh'g en banc denied*, 515 F.3d 1361 (Fed. Cir. 2008), cert. denied, 129 S.Ct. 70 (2008).

15. The PTO's preferred claim language is a "non-transitory computer-readable medium." The Applicant is encouraged to adopt this language to obviate this rejection.

Claim Rejections - 35 USC § 102

16. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

17. Claims 1-33 are rejected under 35 U.S.C. 102(a) and 35 U.S.C. 102(e) as being anticipated by U.S. Patent Application Publication No. 2006/0123244 A1 to Gheorghescu et al., hereinafter Gheorghescu.

18. As per claims 1 and 19, Gheorghescu teaches method and a computer-readable medium comprising instructions for classifying software, said method comprising:

identifying at least one of a functional block and a property of said software (paragraphs 0009, 0034, 0042, i.e. dividing the program code into “basic blocks,” and identifying subsequent basic blocks);

identifying one or more genes in said at least one of a functional block and a property of said software (Figure 4 [step 416], paragraphs 0034, 0038, 0040, i.e. identifying sections of the basic block using signatures or other characteristics of the basic block);

matching said one or more genes against one or more classifications defined by a groupings of genes using a processor (Figure 4 [step 418], paragraphs 0038, 0039);

classifying said software based on said one or more classifications (Figure 4 [steps 420, 422], paragraphs 0039, 0040, i.e. classifying the basic block as being infected with malware based on the signature or other characteristics of the malware); and

notifying a user of said one or more classifications (Figure 4 [step 420], paragraphs 0038, 0039).

Art Unit: 2439

19. Regarding claims 2 and 20, Gheorghescu teaches wherein said classifying step further comprises classifying said software as malware based on said one or more classifications (Figure 4 [step 422], paragraphs 0039, 0040, i.e. classifying the basic block as being infected with malware based on the signature or other characteristics of the malware).

20. Regarding claims 3 and 21, Gheorghescu teaches wherein said classifying step further comprises classifying said software as unwanted software (Figure 4 [step 422], paragraphs 0039, 0040, i.e. classifying the basic block as being infected with malware based on the signature or other characteristics of the malware).

21. Regarding claims 4 and 22, Gheorghescu teaches unpacking said software (paragraph 0038).

22. Regarding claims 5 and 23, Gheorghescu teaches disassembling said software (paragraphs 0009, i.e. dividing the program code into “basic blocks”).

23. Regarding claims 6 and 24, Gheorghescu teaches filtering said software (paragraphs 0042, 0043, i.e. translating the program into safe program code).

24. Regarding claims 7 and 25, Gheorghescu teaches unencrypting said software (paragraph 0038).

Art Unit: 2439

25. Regarding claims 8 and 26, Gheorghescu teaches generating an output based on said classifying of said software (Figure 4 [step 420], paragraphs 0038, 0039).

26. Regarding claims 9 and 27, Gheorghescu teaches disinfecting at least one of said software and a computer when said software is classified as malware (paragraphs 0042, 0043, i.e. translating the program into safe program code).

27. Regarding claims 10 and 28, Gheorghescu teaches removing said software when said software is classified as malware or unwanted software (paragraphs 0042, 0043, i.e. translating the program into safe program code).

28. Regarding claims 11 and 29, Gheorghescu teaches quarantining said software when said software is classified as malware or unwanted software (paragraph 0004).

29. Regarding claims 12 and 30, Gheorghescu teaches generating reports regarding said software (Figure 4 [step 420], paragraphs 0038, 0039).

30. Regarding claims 13 and 31, Gheorghescu teaches blocking access to said software when said software is classified as malware or unwanted software (paragraphs 0042, 0043, i.e. translating the program into safe program code).

31. Regarding claims 14 and 32, Gheorghescu teaches scanning a computer for said software,

Art Unit: 2439

wherein said scanning include user initiated scanning, scheduled scanning and on-access scanning (Figure 4 [step 416], paragraphs 0038, 0040, i.e. identifying sections of the basic block using signatures or other characteristics of the basic block).

32. Regarding claim 15, Gheorghescu teaches wherein said classification is based upon one or more groupings of genes (Figure 4 [step 422], paragraphs 0039, 0040, i.e. classifying the basic block as being infected with malware based on the signature or other characteristics of the malware).

33. As per claim 16, Gheorghescu teaches a method for generating software classifications for use in classifying software, said method comprising:

identifying one or more genes that appear in software (paragraphs 0009, 0034, 0042, i.e. dividing the program code into “basic blocks,” and identifying successor and subsequent basic blocks);

combining a plurality of genes to form a set of genes (paragraph 0034, i.e. identifying successor basic blocks);

testing said set of genes for false-positives against one or more reference files using a processor; (Figure 4 [steps 416, 418], paragraphs 0034, 0038, 0039, 0040, i.e. scanning those basic blocks for malware); and

defining a software classification based on said set of genes (Figure 4 [steps 420, 422], paragraphs 0039, 0040, i.e. classifying the basic block as being infected with malware based on the signature or other characteristics of the malware); and

Art Unit: 2439

returning a result of said software classification based on said set of genes to a user (Figure 4 [step 420], paragraphs 0038, 0039).

34. Regarding claim 17, Gheorghescu teaches wherein said software classification classifies malware (Figure 4 [step 422], paragraphs 0039, 0040, i.e. classifying the basic block as being infected with malware based on the signature or other characteristics of the malware).

35. Regarding claim 18, Gheorghescu teaches wherein said software classification classifies unwanted software (Figure 4 [step 422], paragraphs 0039, 0040, i.e. classifying the basic block as being infected with malware based on the signature or other characteristics of the malware).

36. Regarding claim 33, Gheorghescu teaches a classification generation routine configured to generate software classifications, said classification routine executing the steps of:

identifying a software functionality (paragraphs 0009, 0034, 0042);

defining a characteristic based on said identified software functionality (Figure 4 [step 416], paragraphs 0034, 0038, 0040, i.e. identifying sections of the basic block using signatures or other characteristics of the basic block); and

combining a plurality of characteristics to form a classification (Figure 4 [steps 420, 422], paragraphs 0039, 0040, i.e. classifying the basic block as being infected with malware based on the signature or other characteristics of the malware).

Conclusion

37. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

38. The following patents are cited to further show the state of the art with respect to detecting malicious API and procedure calls in a program, such as:

United States Patent Application Publication No. 2006/0015940 A1 to Zamir et al., which is cited to show detecting malicious API calls in a computer program.

United States Patent Application Publication No. 2005/0187740 A1 to Marinescu, which is cited to show generating behavior signatures of API calls and comparing them to known malware signatures.

United States Patent No. 7,814,544 B1 to Wilhelm, which is cited to show monitoring API calls for malicious behavior.

39. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

40. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Art Unit: 2439

41. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian LaForgia whose telephone number is (571)272-3792.

The examiner can normally be reached on Monday thru Thursday 7-5.

42. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad can be reached on (571) 272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

43. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christian LaForgia/
Primary Examiner, Art Unit 2439

clf

Notice of References Cited	Application/Control No. 11/428,203	Applicant(s)/Patent Under Reexamination GODWOOD ET AL.	
	Examiner Christian LaForgia	Art Unit 2439	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2005/0187740 A1	08-2005	Marinescu, Adrian M.	703/001
*	B	US-2006/0015940 A1	01-2006	Zamir et al.	726/022
*	C	US-7,814,544 B1	10-2010	Wilhelm, Jeffrey	726/22
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L3	1	(US-20060123244-\$).did.	US-PGPUB	OR	OFF	2011/03/07 12:56
L4	1	3 and basic adj block	US-PGPUB; USPAT	OR	ON	2011/03/07 12:56
S1	3	sophos.as.	US-PGPUB; USPAT	OR	ON	2010/05/13 09:11
S2	3	godwood-ben\$.in.	US-PGPUB; USPAT	OR	ON	2010/05/13 09:11
S3	4	mccourt-william\$.in.	US-PGPUB; USPAT	OR	ON	2010/05/13 09:14
S4	2	("20050172338" "20040181677").pn.	US-PGPUB; USPAT	OR	ON	2010/05/13 09:16
S5	5	("2005/0172338").URPN.	USPAT	OR	OFF	2010/05/13 09:21
S6	0	("2004/0181677").URPN.	USPAT	OR	OFF	2010/05/13 09:22
S7	0	("2004/0181677").URPN.	USPAT	OR	OFF	2010/05/13 09:22
S8	1	(anti\$virus (malware virus trojan adware spyware dialer) near detect\$3) same (detect\$3 determin \$5) with (malware malicious trojan adware spyware dialer) with (decompil\$3 disassembl \$3) with (program code)	US-PGPUB; USPAT	OR	ON	2010/05/13 09:25
S9	8	(detect\$3 determin\$5) with (malware malicious trojan adware spyware dialer) with (decompil\$3 disassembl\$3) with (program code)	US-PGPUB; USPAT	OR	ON	2010/05/13 09:27


S10	63	(detect\$3 determin\$5) with (malware malicious trojan adware spyware dialer) with (characteristic) with (program code)	US-PGPUB; USPAT	OR	ON	2010/05/13 09:30
S11	8	(detect\$3 determin\$5) with (malware malicious trojan adware spyware dialer) with (characteristic) with (program code) and (disassembl\$3 unpack\$3)	US-PGPUB; USPAT	OR	ON	2010/05/13 09:31
S13	3	("2006/0123244").URPN.	USPAT	OR	OFF	2010/05/13 11:20
S14	11	((("20050005153") or ("20040041315") or ("5381533") or ("5765030") or ("20020091934") or ("6704925") or ("5826013") or ("5951698") or ("6357008") or ("20030101381") or ("6637514")).PN.	US-PGPUB; USPAT	OR	OFF	2010/05/13 11:28
S15	77	("6357008").URPN.	USPAT	OR	OFF	2010/05/13 11:30
S16	74	("5826013").URPN.	USPAT	OR	OFF	2010/05/13 11:38
S17	1	(US-20060123244-\$.did.	US-PGPUB	OR	OFF	2010/05/13 12:22
S18	1	S17 and quarantin\$3	US-PGPUB; USPAT	OR	ON	2010/05/13 12:22
S19	18	726/24.ccls. and program with API near call	US-PGPUB; USPAT	OR	OFF	2011/03/07 11:49
S20	29	(scan\$4 check\$3 determin\$5 detect\$3) with API near call with (malware malicious virus trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2011/03/07 11:52
S21	3	("20040181677" "20050172338" "20090187992").pn.	US-PGPUB; USPAT	OR	OFF	2011/03/07 12:04

S22	13	726/24.ccls. and gene	US- PGPUB; USPAT	OR	ON	2011/03/07 12:06
-----	----	-----------------------	------------------------	----	----	---------------------

EAST Search History (Interference)


Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S12	1	sophos.as.	USPAT; UPAD	OR	ON	2010/05/13 09:11

3/ 7/ 11 1:09:42 PM**C:\ Documents and Settings\ claforgia\ My Documents\ EAST\ Workspaces\ 11428203.wsp**

<i>Index of Claims</i> 	Application/Control No. 11428203	Applicant(s)/Patent Under Reexamination GODWOOD ET AL.
	Examiner Christian LaForgia	Art Unit 2439

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

<input type="checkbox"/> Claims renumbered in the same order as presented by applicant				<input type="checkbox"/> CPA				<input type="checkbox"/> T.D.				<input type="checkbox"/> R.1.47			
CLAIM		DATE													
Final	Original	05/14/2010	03/07/2011												
	1	✓	✓												
	2	✓	✓												
	3	✓	✓												
	4	✓	✓												
	5	✓	✓												
	6	✓	✓												
	7	✓	✓												
	8	✓	✓												
	9	✓	✓												
	10	✓	✓												
	11	✓	✓												
	12	✓	✓												
	13	✓	✓												
	14	✓	✓												
	15	✓	✓												
	16	✓	✓												
	17	✓	✓												
	18	✓	✓												
	19	✓	✓												
	20	✓	✓												
	21	✓	✓												
	22	✓	✓												
	23	✓	✓												
	24	✓	✓												
	25	✓	✓												
	26	✓	✓												
	27	✓	✓												
	28	✓	✓												
	29	✓	✓												
	30	✓	✓												
	31	✓	✓												
	32	✓	✓												
	33	✓	✓												

Search Notes 	Application/Control No. 11428203	Applicant(s)/Patent Under Reexamination GODWOOD ET AL.
	Examiner Christian LaForgia	Art Unit 2439

SEARCHED			
Class	Subclass	Date	Examiner
none	none	5/13/10	clf
726	24	3/7/11	clf

SEARCH NOTES		
Search Notes	Date	Examiner
EAST search - see enclosed	5/13/10	clf
IEEE search	5/13/10	clf
ACM search	5/13/10	clf
Google search	5/13/10	clf
Inventor search	5/13/10	clf
Assignee search	5/13/10	clf
updated EAST - see enclosed	3/7/11	clf

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

	/Christian LaForgia/ Primary Examiner.Art Unit 2439
--	--

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449A/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Complete if Known</i>	
				Application Number	11/428,203
				Filing Date	Jun 30, 2006
				First Named Inventor	Benjamin John Godwood
				Art Unit	2439
				Examiner Name	LAFORGIA, Christian A.
Sheet	1	of	1	Attorney Docket No: SPHS-0007-P01	

US PATENT DOCUMENTS					
Examiner Initial *	Cite No	Document Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
/CLF/		2004/0181677	Sep 16, 2004	Hong, Man-Pyo et al.	
/CLF/		2005/0172338	Aug 4, 2005	Sandu, Catalin D., et al.	
/CLF/		20090187992A1	Jul 23, 2009	Poston, R. J.	

FOREIGN PATENT DOCUMENTS						
Examiner Initials*	Cite No	Foreign Patent Document	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T ²

OTHER DOCUMENTS -- NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T ²
/CLF/	NPL-8	, "Intellectual Property Office-PGB Search Report", 9/27/10, all	
/CLF/	NPL-7	SKORMIN, et al., ""In The Search of the "Gene of Replication" in Malicious Codes"", <u>Proceedings from the Sixth Annual IEEE Systems, Man and Cybernetics Information Assurance Workshop</u> 2005, 193-200	

EXAMINER

/Christian LaForgia/

DATE CONSIDERED

03/07/2011

S/N 11/428,203

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Ben Godwood

Examiner: Christian A. Laforgia

Serial No.: 11/428,203

Group Art Unit: 2439

Filed: June 30, 2006

Docket No.: SPHS-0007-P01

Title: METHOD AND SYSTEM FOR CLASSIFICATION OF SOFTWARE USING
CHARACTERISTICS AND COMBINATIONS OF SUCH
CHARACTERISTICS

NON-COMPLIANT AMENDMENT RESPONSE
AND
AMENDMENT AND RESPONSE UNDER 37 C.F.R. § 1.111

Mail Stop Amendment
Commissioner for Patents
PO Box 1450
Alexandria, Virginia 22313-1450

Sir:

Applicants have reviewed the Office Action mailed on May 17, 2010 ("Office Action"). Additionally, this response corrects the items indicated in the Notice of Non-Compliant Amendment mailed September 22, 2010. This response is accompanied by a petition, as well as the appropriate fee, to obtain a three-month extension of the period for responding to the Notice of Non-Compliant Amendment mailed 9/22/2010, thereby moving the deadline for response from 10/22/2010 to 01/22/2011 (next business day 1/24/2011).

A request for extension of time appears on Page 2 of this Response.

A listing of the claims appears on Page 3 of this Response.

An amendment to the specification appears on Page 8 of this Response.

Remarks begin on Page 9 of this response.

REQUEST FOR EXTENSION OF TIME

Applicant respectfully requests that the time for responding to the outstanding non-compliant amended be extended for three month from October 22, 2010 to January 22, 2011 (next business day January 24, 2011). A fee of \$1110.00 as specified by 37 C.F.R 1.17(a)(3) for a large entity accompanies this request.

AMENDMENT TO THE CLAIMS

This listing of claims will replace all the prior versions of the claims in the applications.

1. (Currently Amended) A method for classifying software, said method comprising;
identifying at least one of a functional block and a property of said software;
identifying one or more genes in said at least one of a functional block and a property of said software;
matching said one or more genes against one or more classifications defined by a groupings of genes using a processor; and
classifying said software based on said one or more classifications; and
notifying a user of said one or more classifications.
2. (Original) The method of claim 1, wherein said classifying step further comprises classifying said software as malware based on said one or more classifications.
3. (Original) The method of claim 1, wherein said classifying step further comprises classifying said software as unwanted software.
4. (Original) The method of claim 1, further comprising unpacking said software.
5. (Original) The method of claim 1, further comprising disassembling said software.
6. (Original) The method of claim 1, further comprising filtering said software.
7. (Original) The method of claim 1, further comprising unencrypting said software.
8. (Original) The method of claim 1, further comprising generating an output based on said classifying of said software.

9. (Original) The method of claim 1, further comprising disinfecting at least one of said software and a computer when said software is classified as malware.

10. (Original) The method of claim 1, further comprising removing said software when said software is classified as malware or unwanted software.

11. (Original) The method of claim 1, further comprising quarantining said software when said software is classified as malware or unwanted software.

12. (Original) The method of claim 1, further comprising generating reports regarding said software.

13. (Original) The method of claims 1, further comprising blocking access to said software when said software is classified as malware or unwanted software.

14. (Original) The method of claim 1, further comprising scanning a computer for said software, wherein said scanning include user initiated scanning, scheduled scanning and on-access scanning.

15. (Original) The method of claim 1, wherein said classification is based upon one or more groupings of genes.

16. (Currently Amended) A method for generating software classifications for use in classifying software, said method comprising:

- identifying one or more genes that appear in software;
- combining a plurality of genes that appear in software;
- testing said set of genes for false-positives against one or more reference files using a processor; and
- defining a software classification based on said set of genes; and
returning a result of said software classification based on said set of genes to a user.

17. (Original) The method of claim 16, wherein said software classification classifies malware.

18. (Original) The method of claim 16, wherein said software classification classifies unwanted software.

19. (Currently Amended) A computer-readable medium having a set of instructions for execution on a computer, said set of instructions comprising:

an identification routine configured to identify one or more functional blocks and/or properties of software;

a routine configured to identify genes in said one or more functional blocks and/or properties;

a matching routine configured to match genes against a list of predetermined classifications defined by groupings of genes using a processor; ~~and~~

a classification routine configured to classify said software; and

a reporting routine configured to report said classifying of said software.

20. (Original) The set of instructions of claim 19, wherein said classification routine is configured to classify malware.

21. (Original) The set of instructions of claim 19, wherein said classification routine is configured to classify unwanted software.

22. (Original) The set of instructions of claim 19, further comprising an unpacking routine configured to unpack said software.

23. (Original) The set of instructions of claim 19, further comprising a disassembly routine configured to disassemble said software.

24. (Original) The set of instructions of claim 19, further comprising a filtering routine configured to filter said software.

25. (Original) The set of instructions of claim 19, further comprising an unencryption routine configured to unencrypt said software.

26. (Original) The set of instructions of claim 19, further comprising an output routine configured to generate an output based on a classification of said software.

27. (Original) The set of instructions of claim 19, further comprising a disinfection routine configured to disinfect said software when said software is classified as malware.

28. (Original) The set of instructions of claim 19, further comprising a removal routine configured to removed said software when said software is classified as malware or unwanted software.

29. (Original) The set of instructions of claim 19, further comprising a quarantine routine configured to quarantine of said software when said software is classified as malware or unwanted software.

30. (Original) The set of instructions of claim 19, further comprising a reporting routine configured to generate reports regarding said software.

31. (Original) The set of instructions of claim 19, further comprising a blocking routine configured to block access to said software when said software is classified as malware or unwanted software.

32. (Original) The set of instructions of claim 19, further comprising a scanning routine configured to scan a computer for said software, said scanning including at least one of user initiated scanning, scheduled scanning and on-access scanning.

33. (Original) The set of instructions of claim 19, further comprising a classification generation routine configured to generate software classifications, said classification routine executing the steps of:

identifying a software functionality;

defining a characteristic based on said identified software functionality; and

combining a plurality of characteristics to form a classification.

AMENDMENT TO THE SPECIFICATION

Please amend the specification by adding the paragraphs below.

[53] The techniques described herein may be implemented by various means. For example, these techniques may be implemented in hardware, firmware, software, or a combination thereof. For a hardware implementation, the processing units at a transmitter may be implemented within one or more application specific integrated circuits (ASICs), digital signal processors (DSPs), digital signal processing devices (DSPDs), programmable logic devices (PLDs), field programmable gate arrays (FPGAs), processors, controllers, micro-controllers, microprocessors, electronic devices, other electronic units designed to perform the functions described herein, or a combination thereof. The processing units at a receiver may also be implemented within one or more ASICs, DSPs, processors, and so on.

[54] For a software implementation, the techniques may be implemented with instructions (*e.g.*, procedures, functions, and so on) that perform the functions described herein. The instructions may be stored in a memory and executed by a processor. The memory may be implemented within the processor or external to the processor.

[55] The steps of a method or algorithm described in connection with the embodiments disclosed herein may be embodied directly in hardware, in a software module executed by a processor, or in a combination of the two. A software module may reside in RAM memory, flash memory, ROM memory, EPROM memory, EEPROM memory, registers, hard disk, a removable disk, a CD-ROM, or any other form of storage medium known in the art. An exemplary storage medium is coupled to the processor such that the processor can read information from, and write information to, the storage medium. In the alternative, the storage medium may be integral to the processor. The processor and the storage medium may reside in an ASIC. The ASIC may reside in a user terminal. In the alternative, the processor and the storage medium may reside as discrete components in a user terminal.

REMARKS

Information Disclosure Statement

Applicants note that the Examiner has considered the Information Disclosure Statement filed on July 7, 2008.

Specification

The Examiner objected to the specification as failing to provide proper antecedent basis for the claimed subject matter of claims 19-33. The Examiner states that the specification fails to define the term “computer readable medium” and required correction. Applicants have amended the specification to define the term “computer readable medium” and respectfully requests that the objection be withdrawn.

Claim Rejections- 35 USC§ 101

Claims 1-18 were rejected under 35 U.S.C. § 101 as not falling within one of the four statutory categories of invention. While the claims recite a series of steps or acts to be performed, a statutory “process” under 35 U.S.C. § 101 must satisfy the “machine-or-transformation” test. The Examiner states that the method steps are broad enough that the claim could be completely performed mentally, verbally, or without a machine, nor is any transformation evident.

Applicants have amended claims 1 and 16 to specify “matching said one or more genes against one or more classifications defined by a grouping of genes using a processor” and “notifying a user of said one or more classifications” and respectfully submit that the amended claims satisfy the machine-or-transformation test.

In addition, Applicants respectfully submit that the mere application of the machine-or-transformation test is insufficient to make a *prima facie* rejection under 35 U.S.C. § 101. Notably, the Supreme Court has recently rejected the notion that a claim must pass the so-called machine-or-transformation test. *Bilski v. Kappos*, (Supreme Court 2010) (08-964). While the machine-or-transformation test remains an important clue in determining patent eligibility,

passing the test is no longer dispositive. Moreover, Applicants' claims comply with 35 U.S.C. § 101 because the claims are not directed to abstract ideas, laws of nature, or natural phenomena. Thus, even if claims 1 and 16 do not satisfy the machine-or-transformation test, the rejection would still have to be withdrawn since the claims recite patentable subject matter that is not directed to abstract ideas, laws of nature, or physical phenomena.

Since claims 2-15, 17, and 18 depend directly from independent claims 1 and 16, claims 2-15, 17, and 18 are also in condition for allowance. Applicants request that the Examiner withdraw the rejections to claims 1-18.

Claims 19-33 were rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter. The Examiner stated that paragraph 20 of the specification describes that the invention could be implemented in a distributed computer network and that one of ordinary skill in the art could interpret this as defining computer-readable medium to include communication networks. Applicants have amended the specification to clarify the meaning of "computer-readable medium" as noted above and have amended claim 19 to include "a reporting routine configured to report said classifying said software." Applicants respectfully request that the rejection to claims 19-33 be withdrawn.

Claim Rejections – 35 USC § 102

Claims 1-33 were rejected under 35 U.S.C. § 102(e) as being anticipated by Gheorghescu et al, U.S. Patent Publication 2006/0123244 (hereinafter "Gheorghescu"). Applicants traverse this rejection as set forth below.

Claim 1 includes the limitations "identifying one or more genes in said at least one of a functional block and a property of said software"; "matching said one or more genes against one or more classifications defined by a grouping of genes using a processor"; "classifying said software based on said one or more classifications." Applicants respectfully submit that these limitations are not found in the Gheorghescu reference.

Gheorghescu discloses translating blocks of program code that have been scanned and found to contain malware, into code that can be safely executed. The level of scrutiny is limited

to the basic block, and individual elements of functionality are not directly analyzed. The program is broken into “basic blocks” and the blocks are then scanned for malware, and if malware is found, the blocks are translated. This is in contrast to the present invention where a gene is a piece of functionality or a property of the program. The genes are matched against functional blocks of code and the functionality is determined by matching sequences of API calls and the strings that are references.

An additional difference between the present invention and Gheorghescu is that the present invention looks at all functional elements of the program as part of the process of identifying malware and non-malware functionality. Gheorghescu limits the translation activity to the basic blocks that were found to be likely to contain malware during the scan operation. This is different from the present invention, which examines all program functionality.

Because Gheorghescu does not disclose the limitations ““identifying one or more genes in said at least one of a functional block and a property of said software”; “matching said one or more genes against one or more classifications defined by a grouping of genes using a processor”; “classifying said software based on said one or more classifications” Applicants respectfully submit that claim 1 is not anticipated by Gheorghescu.

Claim 19 is allowable for the reasons given above for claim 1.

Claims 2 and 20 are allowable as depending directly from an allowable base claim.

Claims 3 and 21 are allowable as depending directly from an allowable base claim.

Claims 4 and 22 are allowable as depending directly from an allowable base claim.

Claims 5 and 23 are allowable as depending directly from an allowable base claim.

Claims 6 and 24 are allowable as depending directly from an allowable base claim.

Claims 7 and 25 are allowable as depending directly from an allowable base claim.

Claims 8 and 26 are allowable as depending directly from an allowable base claim.

Claims 9 and 27 are allowable as depending directly from an allowable base claim.

Claims 10 and 28 are allowable as depending directly from an allowable base claim.

Claims 11 and 29 are allowable as depending directly from an allowable base claim.

Claims 12 and 30 are allowable as depending directly from an allowable base claim.

Claims 13 and 31 are allowable as depending directly from an allowable base claim.

Claims 14 and 32 are allowable as depending directly from an allowable base claim.

Claim 15 is allowable as depending directly from an allowable base claim.

Claim 16 is allowable for the reasons given above. In addition, claim 16 is allowable for the reasons given below. In the rejection, the Examiner cites Gheorghescu, paragraph 0034 as disclosing “combining a plurality of genes to form a set of genes.” Applicants respectfully disagree. Paragraph 0034 discloses the idea of identifying successor basic blocks. This merely identifies the order of performing tasks within the program. In contrast, in the Applicants’ invention, genes are a smaller piece of the functionality of the program and direct the processor to perform certain tasks or operations. Genes may be independent of the successive order in which operations are performed, and may cross multiple functional blocks of executable code.

Furthermore, Gheorghescu is silent regarding “testing said set of genes for false-positives against one or more reference files” as found in amended claim 16. Gheorghescu merely scans the program for malware. Scanning is not the same as testing the code. Applicants’ invention examines functionality, not heuristics, as is the case with Gheorghescu. Therefore, Applicants respectfully submit that claim 16 is allowable over the cited prior art reference, Gheorghescu.

Claim 17 is allowable as depending directly from an allowable base claim.

Claim 18 is allowable as depending directly from an allowable base claim.

Claim 33 is allowable as depending directly from an allowable base claim.

CONCLUSION

For all of the foregoing reasons, Applicants believe that the claims are in condition for allowance and such notice is respectfully requested. Allowance is earnestly solicited, and the Examiner is requested to contact the undersigned in case of any questions relating to this matter. Further, it is believed that the pending claims have been addressed. However, absence to reply to any specific rejection, objection, or comment does not signify agreement with or concession of that rejection, objection, or comment.

No additional fees are believed to be required with this paper. However, the Director is hereby authorized to charge any fees under 37 C.F.R. §§1.16 and 1.17, or to credit any overpayments, to Deposit Account No. 50-4262.

Respectfully submitted,

STRATEGIC PATENTS, P.C.

/Robert Mazzaresse/

Robert A. Mazzaresse

Reg. No. 42,852

Telephone: 781-453-9993

Customer Number 43520

January 24, 2011

Electronic Patent Application Fee Transmittal

Application Number:	11428203			
Filing Date:	30-Jun-2006			
Title of Invention:	METHOD AND SYSTEM FOR CLASSIFICATION OF SOFTWARE USING CHARACTERISTICS AND COMBINATIONS OF SUCH CHARACTERISTICS			
First Named Inventor/Applicant Name:	Ben Godwood			
Filer:	John H. Nortrop			
Attorney Docket Number:	SPHS-0007-P01			
Filed as Large Entity				
Utility under 35 USC 111(a) Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 3 months with \$0 paid	1253	1	1110	1110

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Total in USD (\$)				1110

Electronic Acknowledgement Receipt

EFS ID:	9287006
Application Number:	11428203
International Application Number:	
Confirmation Number:	3669
Title of Invention:	METHOD AND SYSTEM FOR CLASSIFICATION OF SOFTWARE USING CHARACTERISTICS AND COMBINATIONS OF SUCH CHARACTERISTICS
First Named Inventor/Applicant Name:	Ben Godwood
Customer Number:	43520
Filer:	John H. Nortrop
Filer Authorized By:	
Attorney Docket Number:	SPHS-0007-P01
Receipt Date:	24-JAN-2011
Filing Date:	30-JUN-2006
Time Stamp:	10:24:41
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$1110
RAM confirmation Number	10041
Deposit Account	504262
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		SPHS-0007-P01_012411_Non-CompliantResponse.pdf	152257 b9a5d73991e592e84dc2092c8cb5f94b509146c9	yes	13
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Amendment/Req. Reconsideration-After Non-Final Reject		1	1	
	Extension of Time		2	2	
	Claims		3	7	
	Specification		8	8	
	Applicant Arguments/Remarks Made in an Amendment		9	13	
Warnings:					
Information:					
2	Fee Worksheet (PTO-875)	fee-info.pdf	30509 0b1c27a90ef440fa4ebec9eba74d1b81bb87d960	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			182766		
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875					Application or Docket Number 11/428,203		Filing Date 06/30/2006		<input type="checkbox"/> To be Mailed	
APPLICATION AS FILED – PART I										
(Column 1)			(Column 2)			SMALL ENTITY <input type="checkbox"/> OR		OTHER THAN SMALL ENTITY		
FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)	OR	RATE (\$)	FEE (\$)			
<input type="checkbox"/> BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A				
<input type="checkbox"/> SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A			N/A				
<input type="checkbox"/> EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A				
TOTAL CLAIMS (37 CFR 1.16(j))	minus 20 =	*	X \$	=		X \$	=			
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X \$	=		X \$	=			
<input type="checkbox"/> APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).									
<input type="checkbox"/> MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))										
			TOTAL			TOTAL				
* If the difference in column 1 is less than zero, enter "0" in column 2.										
APPLICATION AS AMENDED – PART II										
(Column 1)			(Column 2)			SMALL ENTITY OR		OTHER THAN SMALL ENTITY		
AMENDMENT	01/24/2011	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	OR	RATE (\$)	ADDITIONAL FEE (\$)
	Total (37 CFR 1.16(i))	* 33	Minus	** 33	= 0	X \$	=		X \$	= 0
	Independent (37 CFR 1.16(h))	* 3	Minus	*** 3	= 0	X \$	=		X \$	= 0
	<input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))									
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))									
						TOTAL ADD'L FEE			TOTAL ADD'L FEE	0
(Column 1)			(Column 2)			SMALL ENTITY OR		OTHER THAN SMALL ENTITY		
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	OR	RATE (\$)	ADDITIONAL FEE (\$)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X \$	=		X \$	=
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X \$	=		X \$	=
	<input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))									
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))									
						TOTAL ADD'L FEE			TOTAL ADD'L FEE	
<p>* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.</p> <p>** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".</p> <p>*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".</p> <p>The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.</p>										

Legal Instrument Examiner:
/ERIC DAVIS/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449A/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary)				<i>Complete if Known</i>	
				Application Number	11/428,203
				Filing Date	Jun 30, 2006
				First Named Inventor	Benjamin John Godwood
				Art Unit	2439
				Examiner Name	LAFORGIA, Christian A.
Sheet	1	of	1	Attorney Docket No: SPHS-0007-P01	

US PATENT DOCUMENTS					
Examiner Initial *	Cite No	Document Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		2004/0181677	Sep 16, 2004	Hong, Man-Pyo et al.	
		2005/0172338	Aug 4, 2005	Sandu, Catalin D., et al.	
		20090187992A1	Jul 23, 2009	Poston, R. J.	

FOREIGN PATENT DOCUMENTS						
Examiner Initials*	Cite No	Foreign Patent Document	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T ²

OTHER DOCUMENTS -- NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T ²
	NPL-8	, "Intellectual Property Office-PGB Search Report", 9/27/10 , all	
	NPL-7	SKORMIN, et al., ""In The Search of the "Gene of Replication" in Malicious Codes"" , <u>Proceedings from the Sixth Annual IEEE Systems, Man and Cybernetics Information Assurance Workshop</u> 2005 , 193-200	

EXAMINER

DATE CONSIDERED

Electronic Patent Application Fee Transmittal

Application Number:	11428203			
Filing Date:	30-Jun-2006			
Title of Invention:	METHOD AND SYSTEM FOR CLASSIFICATION OF SOFTWARE USING CHARACTERISTICS AND COMBINATIONS OF SUCH CHARACTERISTICS			
First Named Inventor/Applicant Name:	Ben Godwood			
Filer:	John H. Nortrop/Elizabeth Nortrup			
Attorney Docket Number:	SPHS-0007-P01			
Filed as Large Entity				
Utility under 35 USC 111(a) Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
Total in USD (\$)				180

Electronic Acknowledgement Receipt

EFS ID:	9077980
Application Number:	11428203
International Application Number:	
Confirmation Number:	3669
Title of Invention:	METHOD AND SYSTEM FOR CLASSIFICATION OF SOFTWARE USING CHARACTERISTICS AND COMBINATIONS OF SUCH CHARACTERISTICS
First Named Inventor/Applicant Name:	Ben Godwood
Customer Number:	43520
Filer:	John H. Nortrop/Elizabeth Nortrup
Filer Authorized By:	John H. Nortrop
Attorney Docket Number:	SPHS-0007-P01
Receipt Date:	20-DEC-2010
Filing Date:	30-JUN-2006
Time Stamp:	17:25:14
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$ 180
RAM confirmation Number	4966
Deposit Account	504262
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
-----------------	----------------------	-----------	----------------------------------	------------------	------------------

1	Transmittal Letter	SPHS-0007- P01_122010_IDSCommunicati on.pdf	90785 941fc9302ac5f0e14c10653d2f1a015b4f3ef 882	no	2
Warnings:					
Information:					
2	Information Disclosure Statement (IDS) Filed (SB/08)	SPHS-0007- P01_122010_Form1449.pdf	131947 95ccb45b19e46988a918c6f4a3f2093bcd19 ed5a	no	1
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
3	NPL Documents	NPL-7_Skormin- InSearchoftheGene_081810.pdf	1487952 f042fb3eefc269de8aca4ec5c44395b7a48e 77c	no	8
Warnings:					
Information:					
4	NPL Documents	NPL-8_SPHS-0007- PGB_100510_OAreport.pdf	163519 dcf00c175ef461b64f72fb326e0692f879105 c1d	no	3
Warnings:					
Information:					
5	Fee Worksheet (PTO-875)	fee-info.pdf	30701 9a6996dfc15b5c005c88516fadfebaf3106d 7f59	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			1904904		
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Serial No.: 11/428,203
Filing Date: June 30, 2006
Applicant: Benjamin John Godwood et al.
Title: METHOD AND SYSTEM FOR CLASSIFICATION OF SOFTWARE
USING CHARACTERISTICS AND COMBINATIONS OF SUCH
CHARACTERISTICS
Group Art Unit: 2439
Examiner: LAFORGIA, Christian A.
Conf. No.: 3669

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

In compliance with the duty imposed by 37 C.F.R. § 1.56, and in accordance with 37 C.F.R. §§ 1.97 *et seq.*, the referenced materials are brought to the attention of the Examiner for consideration in connection with the above-identified patent application. Applicant respectfully requests that this Supplemental Information Disclosure Statement be entered and the documents listed on the attached Form 1449 be considered by the Examiner and made of record. Pursuant to the provisions of MPEP 609, Applicant requests that a copy of the 1449 form, initialed as being considered by the Examiner, be returned to the Applicant with the next official communication.

Pursuant to 37 C.F.R. §1.97(c)(2), Applicants hereby authorize the Commissioner to charge the fee of \$180.00 as set forth in 37 C.F.R. §1.17(p), to Deposit Account No. 50-4262. Please charge any additional fees or credit any overpayment to Deposit Account No. 50-4262.

Pursuant to 37 C.F.R. 1.98(a)(2), Applicant believes that copies of cited U.S. Patents and Published and Non-Published Applications identifiable by USPTO Serial Number are no longer required to be provided to the Office. Notification of this change to this effect was provided in

-2-

the United States Patent and Trademark Office OG Notices dated October 12, 2004 and October 19, 2004. Thus, Applicant has not included copies of any US Patents or US Patent Applications identifiable by serial number that may be cited with this submission. Should the Office require copies to be provided, Applicant respectfully requests that notice of such requirement be directed to Applicant's below-signed representative. Applicant acknowledges the requirement to submit copies of foreign patent documents and non-patent literature in accordance with 37 C.F.R. 1.98(a)(2).

The Examiner is invited to contact the Applicant's Representative at the below-listed telephone number if there are any questions regarding this communication.

Respectfully submitted on December 20, 2010,

STRATEGIC PATENTS, P.C.

/John H. Nortrup, Reg. No. 59,063/

John H. Nortrup

Telephone: 207-985-2126

Customer Number 43520

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875					Application or Docket Number 11/428,203		Filing Date 06/30/2006		<input checked="" type="checkbox"/> To be Mailed	
APPLICATION AS FILED – PART I										
(Column 1)			(Column 2)		SMALL ENTITY <input type="checkbox"/>		OR		OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)	RATE (\$)	FEE (\$)				
<input type="checkbox"/> BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A		N/A					
<input type="checkbox"/> SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A		N/A					
<input type="checkbox"/> EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A		N/A					
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X \$	=	OR	X \$	=			
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X \$	=		X \$	=			
<input type="checkbox"/> APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).									
<input type="checkbox"/> MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))										
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL				
APPLICATION AS AMENDED – PART II										
(Column 1)			(Column 2)		(Column 3)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY	
AMENDMENT	09/17/2010	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	RATE (\$)	ADDITIONAL FEE (\$)		
	Total (37 CFR 1.16(i))	* 33	Minus	** 33	= 0	X \$ =	OR	X \$52=	0	
	Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X \$ =	OR	X \$220=	0	
	<input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))									
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))									
						TOTAL ADD'L FEE		TOTAL ADD'L FEE	0	
AMENDMENT	Total (37 CFR 1.16(i))	*	Minus	**	=	X \$ =	OR	X \$ =		
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X \$ =	OR	X \$ =		
	<input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))									
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))									
						TOTAL ADD'L FEE		TOTAL ADD'L FEE		
<p>* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.</p> <p>** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".</p> <p>*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".</p> <p>The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.</p>										

Legal Instrument Examiner:
/NICHELE PETERSON/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



UNITED STATES PATENT AND TRADEMARK OFFICE


UNITED STATES DEPARTMENT OF COMMERCE U.S. Patent and Trademark Office

Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

43520 e 09/22/2010

STRATEGIC PATENTS P.C..
C/O PORTFOLIOIP
P.O. BOX 52050
MINNEAPOLIS, MN 55402

Paper No.

Application No.:	11/428,203 	Date Mailed:	09/22/2010
First Named Inventor:	Godwood, Ben,	Examiner:	LAFORGIA, CHRISTIAN A
Attorney Docket No.:	SPHS-0007-P01	Art Unit:	2439
Confirmation No.:	3669	Filing Date:	06/30/2006

Please find attached an Office communication concerning this application or proceeding.

Commissioner for Patents

Notice of Non-Compliant Amendment (37 CFR 1.121)	Application No. 11/428,203	Applicant(s) GODWOOD ET AL.	
		Art Unit 2600	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

The amendment document filed on 17 September, 2010 is considered non-compliant because it has failed to meet the requirements of 37 CFR 1.121 or 1.4. In order for the amendment document to be compliant, correction of the following item(s) is required.

THE FOLLOWING MARKED (X) ITEM(S) CAUSE THE AMENDMENT DOCUMENT TO BE NON-COMPLIANT:

- ☒ 1. Amendments to the specification:
 - ☐ A. Amended paragraph(s) do not include markings.
 - ☒ B. New paragraph(s) should not be underlined.
 - ☐ C. Other _____.
- ☐ 2. Abstract:
 - ☐ A. Not presented on a separate sheet. 37 CFR 1.72.
 - ☐ B. Other _____.
- ☐ 3. Amendments to the drawings:
 - ☐ A. The drawings are not properly identified in the top margin as "Replacement Sheet," "New Sheet," or "Annotated Sheet" as required by 37 CFR 1.121(d).
 - ☐ B. The practice of submitting proposed drawing correction has been eliminated. Replacement drawings showing amended figures, without markings, in compliance with 37 CFR 1.84 are required.
 - ☐ C. Other _____.
- ☒ 4. Amendments to the claims:
 - ☐ A. A complete listing of all of the claims is not present.
 - ☐ B. The listing of claims does not include the text of all pending claims (including withdrawn claims)
 - ☐ C. Each claim has not been provided with the proper status identifier, and as such, the individual status of each claim cannot be identified. Note: the status of every claim must be indicated after its claim number by using one of the following status identifiers: (Original), (Currently amended), (Canceled), (Previously presented), (New), (Not entered), (Withdrawn) and (Withdrawn-currently amended).
 - ☐ D. The claims of this amendment paper have not been presented in ascending numerical order.
 - ☐ E. Other: _____.
- ☐ 5. Other (e.g., the amendment is unsigned or not signed in accordance with 37 CFR 1.4): For further explanation of the amendment format required by 37 CFR 1.121, see MPEP § 714.

TIME PERIODS FOR FILING A REPLY TO THIS NOTICE:

1. Applicant is given **no new time period** if the non-compliant amendment is an after-final amendment or an amendment filed after allowance, or a drawing submission (only) If applicant wishes to resubmit the non-compliant after-final amendment with corrections, the **entire corrected amendment** must be resubmitted.
2. Applicant is given **one month**, or thirty (30) days, whichever is longer, from the mail date of this notice to supply the correction, if the non-compliant amendment is one of the following: a preliminary amendment, a non-final amendment (including a submission for a request for continued examination (RCE) under 37 CFR 1.114), a supplemental amendment filed within a suspension period under 37 CFR 1.103(a) or (c), and an amendment filed in response to a Quayle action. If any of above boxes 1 to 4 are checked, the correction required is only the corrected section of the non-compliant amendment in compliance with 37 CFR 1.121.

Extensions of time are available under 37 CFR 1.136(a) only if the non-compliant amendment is a non-final amendment or an amendment filed in response to a Quayle action.

Failure to timely respond to this notice will result in:

Abandonment of the application if the non-compliant amendment is a non-final amendment or an amendment filed in response to a Quayle action; or

Non-entry of the amendment if the non-compliant amendment is a preliminary amendment or supplemental amendment.

Legal Instruments Examiner (LIE), if applicable /NICHELE PETERSON/

Telephone No: (571)272-7273

S/N 11/428,203

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Ben Godwood

Examiner: Christian A. Laforgia

Serial No.: 11/428,203

Group Art Unit: 2439

Filed: June 30, 2006

Docket No.: SPHS-0007-P01

Title: METHOD AND SYSTEM FOR CLASSIFICATION OF SOFTWARE USING
CHARACTERISTICS AND COMBINATIONS OF SUCH
CHARACTERISTICS

AMENDMENT AND RESPONSE UNDER 37 C.F.R. § 1.111

Mail Stop Amendment
Commissioner for Patents
PO Box 1450
Alexandria, Virginia 22313-1450

Sir:

Applicants have reviewed the Office Action mailed on May 17, 2010 ("Office Action"). This response is accompanied by a petition, as well as the appropriate fee, to obtain a one-month extension of the period for responding to the Office Action, thereby moving the deadline for response from 08/17/2010 to 09/17/2010.

A request for extension of time appears on Page 2 of this Response.

A listing of the claims appears on Page 3 of this Response.

An amendment to the specification appears on Page 8 of this Response.

Remarks begin on Page 9 of this response.

REQUEST FOR EXTENSION OF TIME

Applicant respectfully requests that the time for responding to the outstanding action be extended for one month from August 17, 2010 to September 17, 2010. A fee of \$130.00 as specified by 37 C.F.R 1.17(a)(1) for a large entity accompanies this request.

AMENDMENT TO THE CLAIMS

This listing of claims will replace all the prior versions of the claims in the applications.

1. (Currently Amended) A method for classifying software, said method comprising;
identifying at least one of a functional block and a property of said software;
identifying one or more genes in said at least one of a functional block and a property of said software;
matching said one or more genes against one or more classifications defined by a groupings of genes using a processor; and
classifying said software based on said one or more classifications; and
notifying a user of said one or more classifications.
2. (Original) The method of claim 1, wherein said classifying step further comprises classifying said software as malware based on said one or more classifications.
3. (Original) The method of claim 1, wherein said classifying step further comprises classifying said software as unwanted software.
4. (Original) The method of claim 1, further comprising unpacking said software.
5. (Original) The method of claim 1, further comprising disassembling said software.
6. (Original) The method of claim 1, further comprising filtering said software.
7. (Original) The method of claim 1, further comprising unencrypting said software.
8. (Original) The method of claim 1, further comprising generating an output based on said classifying of said software.

9. (Original) The method of claim 1, further comprising disinfecting at least one of said software and a computer when said software is classified as malware.

10. (Original) The method of claim 1, further comprising removing said software when said software is classified as malware or unwanted software.

11. (Original) The method of claim 1, further comprising quarantining said software when said software is classified as malware or unwanted software.

12. (Original) The method of claim 1, further comprising generating reports regarding said software.

13. (Original) The method of claims 1, further comprising blocking access to said software when said software is classified as malware or unwanted software.

14. (Original) The method of claim 1, further comprising scanning a computer for said software, wherein said scanning include user initiated scanning, scheduled scanning and on-access scanning.

15. (Original) The method of claim 1, wherein said classification is based upon one or more groupings of genes.

16. (Currently Amended) A method for generating software classifications for use in classifying software, said method comprising:

- identifying one or more genes that appear in software;
- combining a plurality of genes that appear in software;
- testing said set of genes for false-positives against one or more reference files using a processor; and
- defining a software classification based on said set of genes; and
returning a result of said software classification based on said set of genes to a user.

17. (Original) The method of claim 16, wherein said software classification classifies malware.

18. (Original) The method of claim 16, wherein said software classification classifies unwanted software.

19. (Currently Amended) A computer-readable medium having a set of instructions for execution on a computer, said set of instructions comprising:

an identification routine configured to identify one or more functional blocks and/or properties of software;

a routine configured to identify genes in said one or more functional blocks and/or properties;

a matching routine configured to match genes against a list of predetermined classifications defined by groupings of genes using a processor; ~~and~~

a classification routine configured to classify said software; and

a reporting routine configured to report said classifying of said software.

20. (Original) The set of instructions of claim 19, wherein said classification routine is configured to classify malware.

21. (Original) The set of instructions of claim 19, wherein said classification routine is configured to classify unwanted software.

22. (Original) The set of instructions of claim 19, further comprising an unpacking routine configured to unpack said software.

23. (Original) The set of instructions of claim 19, further comprising a disassembly routine configured to disassemble said software.

24. (Original) The set of instructions of claim 19, further comprising a filtering routine configured to filter said software.

25. (Original) The set of instructions of claim 19, further comprising an unencryption routine configured to unencrypt said software.

26. (Original) The set of instructions of claim 19, further comprising an output routine configured to generate an output based on a classification of said software.

27. (Original) The set of instructions of claim 19, further comprising a disinfection routine configured to disinfect said software when said software is classified as malware.

28. (Original) The set of instructions of claim 19, further comprising a removal routine configured to removed said software when said software is classified as malware or unwanted software.

29. (Original) The set of instructions of claim 19, further comprising a quarantine routine configured to quarantine of said software when said software is classified as malware or unwanted software.

30. (Original) The set of instructions of claim 19, further comprising a reporting routine configured to generate reports regarding said software.

31. (Original) The set of instructions of claim 19, further comprising a blocking routine configured to block access to said software when said software is classified as malware or unwanted software.

32. (Original) The set of instructions of claim 19, further comprising a scanning routine configured to scan a computer for said software, said scanning including at least one of user initiated scanning, scheduled scanning and on-access scanning.

33. (Original) The set of instructions of claim 19, further comprising a classification generation routine configured to generate software classifications, said classification routine executing the steps of:

identifying a software functionality;

defining a characteristic based on said identified software functionality; and

combining a plurality of characteristics to form a classification.

AMENDMENT TO THE SPECIFICATION

Please amend the specification by adding the paragraphs below.

[53] The techniques described herein may be implemented by various means. For example, these techniques may be implemented in hardware, firmware, software, or a combination thereof. For a hardware implementation, the processing units at a transmitter may be implemented within one or more application specific integrated circuits (ASICs), digital signal processors (DSPs), digital signal processing devices (DSPDs), programmable logic devices (PLDs), field programmable gate arrays (FPGAs), processors, controllers, micro-controllers, microprocessors, electronic devices, other electronic units designed to perform the functions described herein, or a combination thereof. The processing units at a receiver may also be implemented within one or more ASICs, DSPs, processors, and so on.

[54] For a software implementation, the techniques may be implemented with instructions (e.g., procedures, functions, and so on) that perform the functions described herein. The instructions may be stored in a memory and executed by a processor. The memory may be implemented within the processor or external to the processor.

[55] The steps of a method or algorithm described in connection with the embodiments disclosed herein may be embodied directly in hardware, in a software module executed by a processor, or in a combination of the two. A software module may reside in RAM memory, flash memory, ROM memory, EPROM memory, EEPROM memory, registers, hard disk, a removable disk, a CD-ROM, or any other form of storage medium known in the art. An exemplary storage medium is coupled to the processor such that the processor can read information from, and write information to, the storage medium. In the alternative, the storage medium may be integral to the processor. The processor and the storage medium may reside in an ASIC. The ASIC may reside in a user terminal. In the alternative, the processor and the storage medium may reside as discrete components in a user terminal.

REMARKS

Information Disclosure Statement

Applicants note that the Examiner has considered the Information Disclosure Statement filed on July 7, 2008.

Specification

The Examiner objected to the specification as failing to provide proper antecedent basis for the claimed subject matter of claims 19-33. The Examiner states that the specification fails to define the term “computer readable medium” and required correction. Applicants have amended the specification to define the term “computer readable medium” and respectfully requests that the objection be withdrawn.

Claim Rejections- 35 USC§ 101

Claims 1-18 were rejected under 35 U.S.C. § 101 as not falling within one of the four statutory categories of invention. While the claims recite a series of steps or acts to be performed, a statutory “process” under 35 U.S.C. § 101 must satisfy the “machine-or-transformation” test. The Examiner states that the method steps are broad enough that the claim could be completely performed mentally, verbally, or without a machine, nor is any transformation evident.

Applicants have amended claims 1 and 16 to specify “matching said one or more genes against one or more classifications defined by a grouping of genes using a processor” and “notifying a user of said one or more classifications” and respectfully submit that the amended claims satisfy the machine-or-transformation test.

In addition, Applicants respectfully submit that the mere application of the machine-or-transformation test is insufficient to make a *prima facie* rejection under 35 U.S.C. § 101. Notably, the Supreme Court has recently rejected the notion that a claim must pass the so-called machine-or-transformation test. *Bilski v. Kappos*, (Supreme Court 2010) (08-964). While the machine-or-transformation test remains an important clue in determining patent eligibility,

passing the test is no longer dispositive. Moreover, Applicants' claims comply with 35 U.S.C. § 101 because the claims are not directed to abstract ideas, laws of nature, or natural phenomena. Thus, even if claims 1 and 16 do not satisfy the machine-or-transformation test, the rejection would still have to be withdrawn since the claims recite patentable subject matter that is not directed to abstract ideas, laws of nature, or physical phenomena.

Since claims 2-15, 17, and 18 depend directly from independent claims 1 and 16, claims 2-15, 17, and 18 are also in condition for allowance. Applicants request that the Examiner withdraw the rejections to claims 1-18.

Claims 19-33 were rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter. The Examiner stated that paragraph 20 of the specification describes that the invention could be implemented in a distributed computer network and that one of ordinary skill in the art could interpret this as defining computer-readable medium to include communication networks. Applicants have amended the specification to clarify the meaning of "computer-readable medium" as noted above and have amended claim 19 to include "a reporting routine configured to report said classifying said software." Applicants respectfully request that the rejection to claims 19-33 be withdrawn.

Claim Rejections – 35 USC § 102

Claims 1-33 were rejected under 35 U.S.C. § 102(e) as being anticipated by Gheorghescu et al, U.S. Patent Publication 2006/0123244 (hereinafter "Gheorghescu"). Applicants traverse this rejection as set forth below.

Claim 1 includes the limitations "identifying one or more genes in said at least one of a functional block and a property of said software"; "matching said one or more genes against one or more classifications defined by a grouping of genes using a processor"; "classifying said software based on said one or more classifications." Applicants respectfully submit that these limitations are not found in the Gheorghescu reference.

Gheorghescu discloses translating blocks of program code that have been scanned and found to contain malware, into code that can be safely executed. The level of scrutiny is limited

to the basic block, and individual elements of functionality are not directly analyzed. The program is broken into “basic blocks” and the blocks are then scanned for malware, and if malware is found, the blocks are translated. This is in contrast to the present invention where a gene is a piece of functionality or a property of the program. The genes are matched against functional blocks of code and the functionality is determined by matching sequences of API calls and the strings that are references.

An additional difference between the present invention and Gheorghescu is that the present invention looks at all functional elements of the program as part of the process of identifying malware and non-malware functionality. Gheorghescu limits the translation activity to the basic blocks that were found to be likely to contain malware during the scan operation. This is different from the present invention, which examines all program functionality.

Because Gheorghescu does not disclose the limitations ““identifying one or more genes in said at least one of a functional block and a property of said software”; “matching said one or more genes against one or more classifications defined by a grouping of genes using a processor”; “classifying said software based on said one or more classifications” Applicants respectfully submit that claim 1 is not anticipated by Gheorghescu.

Claim 19 is allowable for the reasons given above for claim 1.

Claims 2 and 20 are allowable as depending directly from an allowable base claim.

Claims 3 and 21 are allowable as depending directly from an allowable base claim.

Claims 4 and 22 are allowable as depending directly from an allowable base claim.

Claims 5 and 23 are allowable as depending directly from an allowable base claim.

Claims 6 and 24 are allowable as depending directly from an allowable base claim.

Claims 7 and 25 are allowable as depending directly from an allowable base claim.

Claims 8 and 26 are allowable as depending directly from an allowable base claim.

Claims 9 and 27 are allowable as depending directly from an allowable base claim.

Claims 10 and 28 are allowable as depending directly from an allowable base claim.

Claims 11 and 29 are allowable as depending directly from an allowable base claim.

Claims 12 and 30 are allowable as depending directly from an allowable base claim.

Claims 13 and 31 are allowable as depending directly from an allowable base claim.

Claims 14 and 32 are allowable as depending directly from an allowable base claim.

Claim 15 is allowable as depending directly from an allowable base claim.

Claim 16 is allowable for the reasons given above. In addition, claim 16 is allowable for the reasons given below. In the rejection, the Examiner cites Gheorghescu, paragraph 0034 as disclosing “combining a plurality of genes to form a set of genes.” Applicants respectfully disagree. Paragraph 0034 discloses the idea of identifying successor basic blocks. This merely identifies the order of performing tasks within the program. In contrast, in the Applicants’ invention, genes are a smaller piece of the functionality of the program and direct the processor to perform certain tasks or operations. Genes may be independent of the successive order in which operations are performed, and may cross multiple functional blocks of executable code.

Furthermore, Gheorghescu is silent regarding “testing said set of genes for false-positives against one or more reference files” as found in amended claim 16. Gheorghescu merely scans the program for malware. Scanning is not the same as testing the code. Applicants’ invention examines functionality, not heuristics, as is the case with Gheorghescu. Therefore, Applicants respectfully submit that claim 16 is allowable over the cited prior art reference, Gheorghescu.

Claim 17 is allowable as depending directly from an allowable base claim.

Claim 18 is allowable as depending directly from an allowable base claim.

Claim 33 is allowable as depending directly from an allowable base claim.

CONCLUSION

For all of the foregoing reasons, Applicants believe that the claims are in condition for allowance and such notice is respectfully requested. Allowance is earnestly solicited, and the Examiner is requested to contact the undersigned in case of any questions relating to this matter. Further, it is believed that the pending claims have been addressed. However, absence to reply to any specific rejection, objection, or comment does not signify agreement with or concession of that rejection, objection, or comment.

No additional fees are believed to be required with this paper. However, the Director is hereby authorized to charge any fees under 37 C.F.R. §§1.16 and 1.17, or to credit any overpayments, to Deposit Account No. 50-4262.

Respectfully submitted,

STRATEGIC PATENTS, P.C.

/Robert Mazzaresse/

Robert A. Mazzaresse

Reg. No. 42,852

Telephone: 781-453-9993

Customer Number 43520

September 17, 2010

Electronic Patent Application Fee Transmittal

Application Number:	11428203			
Filing Date:	30-Jun-2006			
Title of Invention:	METHOD AND SYSTEM FOR CLASSIFICATION OF SOFTWARE USING CHARACTERISTICS AND COMBINATIONS OF SUCH CHARACTERISTICS			
First Named Inventor/Applicant Name:	Ben Godwood			
Filer:	John H. Nortrop			
Attorney Docket Number:	SPHS-0007-P01			
Filed as Large Entity				
Utility under 35 USC 111(a) Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 1 month with \$0 paid	1251	1	130	130

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Total in USD (\$)				130

Electronic Acknowledgement Receipt

EFS ID:	8443919
Application Number:	11428203
International Application Number:	
Confirmation Number:	3669
Title of Invention:	METHOD AND SYSTEM FOR CLASSIFICATION OF SOFTWARE USING CHARACTERISTICS AND COMBINATIONS OF SUCH CHARACTERISTICS
First Named Inventor/Applicant Name:	Ben Godwood
Customer Number:	43520
Filer:	John H. Nortrop
Filer Authorized By:	
Attorney Docket Number:	SPHS-0007-P01
Receipt Date:	17-SEP-2010
Filing Date:	30-JUN-2006
Time Stamp:	15:42:42
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$ 130
RAM confirmation Number	2167
Deposit Account	504262
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		SPHS-0007-P01_091710_NFOAResponse.pdf	152120 6795557d0110011255b7ac38ce25ce031268c066	yes	13
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Amendment/Req. Reconsideration-After Non-Final Reject		1	1	
	Extension of Time		2	2	
	Claims		3	7	
	Specification		8	8	
	Applicant Arguments/Remarks Made in an Amendment		9	13	
Warnings:					
Information:					
2	Fee Worksheet (PTO-875)	fee-info.pdf	30511 fa7af728892e335299ecc3a6c858b791646698d1	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			182631		
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

11/428,203

06/30/2006

Ben Godwood

SPHS-0007-P01

3669

43520 7590 05/17/2010

STRATEGIC PATENTS P.C..
C/O PORTFOLIOIP
P.O. BOX 52050
MINNEAPOLIS, MN 55402

EXAMINER

LAFORGIA, CHRISTIAN A

ART UNIT

PAPER NUMBER

2439

MAIL DATE

DELIVERY MODE

05/17/2010

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 11/428,203	Applicant(s) GODWOOD ET AL.	
	Examiner Christian LaForgia	Art Unit 2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 30 June 2006.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-33 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-33 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 30 June 2006 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date <u>1/7/08</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-33 have been presented for examination.

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted on 07 July 2008 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement has been considered by the examiner.

Specification

3. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter of claims 19-33. The specification fails to define the term "computer-readable medium." See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction is required.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. Claims 1-18 are rejected under 35 U.S.C. 101 as not falling within one of the four statutory categories of invention. While the claims recite a series of steps or acts to be performed, a statutory "process" under 35 U.S.C. 101 must (1) be tied to particular machine, or (2) transform underlying subject matter (such as an article or material) to a different state or thing. *In Re Bilski*, 545 F.3d 943, 954 (Fed. Cir. 2008). The instant claims are neither positively tied to a particular machine that accomplishes the claimed method steps nor transform underlying subject matter, and therefore do not qualify as a statutory process. The method steps are broad enough that the claim could be completely performed mentally, verbally or without a machine nor is any transformation apparent.

Art Unit: 2439

6. Claims 19-33 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Paragraph 29 bridging pages 8 and 9 of the Specification of the instant application describes that the present invention can be implemented in a distributed network where different processes occur on different machines with a communication network to allow sharing of information. One of ordinary skill in the art could reasonably interpret this as defining computer-readable medium to include communication networks, which entail transitory signals. A transitory, propagating signal does not fall within any one of the four categories of patentable subject matter set forth in 35 U.S.C. § 101, and such claims are therefore ineligible for patent protection. *In re Nuijten*, 500 F.3d 1346, 1357 (Fed. Cir. 2007), *reh'g en banc denied*, 515 F.3d 1361 (Fed. Cir. 2008), *cert. denied*, 129 S.Ct. 70 (2008).

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8. Claims 1-33 are rejected under 35 U.S.C. 102(a) and 35 U.S.C. 102(e) as being anticipated by U.S. Patent Application Publication No. 2006/0123244 A1 to Gheorghescu et al., hereinafter Gheorghescu.

9. As per claims 1 and 19, Gheorghescu teaches method and a computer-readable medium comprising instructions for classifying software, said method comprising:

Art Unit: 2439

identifying at least one of a functional block and a property of said software (paragraphs 0009, 0034, 0042, i.e. dividing the program code into “basic blocks,” and identifying subsequent basic blocks);

identifying one or more genes in said at least one of a functional block and a property of said software (Figure 4 [step 416], paragraphs 0034, 0038, 0040, i.e. identifying sections of the basic block using signatures or other characteristics of the basic block);

matching said one or more genes against one or more classifications defined by a groupings of genes (Figure 4 [step 418], paragraphs 0038, 0039); and

classifying said software based on said one or more classifications (Figure 4 [steps 420, 422], paragraphs 0039, 0040, i.e. classifying the basic block as being infected with malware based on the signature or other characteristics of the malware).

10. Regarding claims 2 and 20, Gheorghescu teaches wherein said classifying step further comprises classifying said software as malware based on said one or more classifications (Figure 4 [step 422], paragraphs 0039, 0040, i.e. classifying the basic block as being infected with malware based on the signature or other characteristics of the malware).

11. Regarding claims 3 and 21, Gheorghescu teaches wherein said classifying step further comprises classifying said software as unwanted software (Figure 4 [step 422], paragraphs 0039, 0040, i.e. classifying the basic block as being infected with malware based on the signature or other characteristics of the malware).

Art Unit: 2439

12. Regarding claims 4 and 22, Gheorghescu teaches unpacking said software (paragraph 0038).

13. Regarding claims 5 and 23, Gheorghescu teaches disassembling said software (paragraphs 0009, i.e. dividing the program code into “basic blocks”).

14. Regarding claims 6 and 24, Gheorghescu teaches filtering said software (paragraphs 0042, 0043, i.e. translating the program into safe program code).

15. Regarding claims 7 and 25, Gheorghescu teaches unencrypting said software (paragraph 0038).

16. Regarding claims 8 and 26, Gheorghescu teaches generating an output based on said classifying of said software (Figure 4 [step 420], paragraphs 0038, 0039).

17. Regarding claims 9 and 27, Gheorghescu teaches disinfecting at least one of said software and a computer when said software is classified as malware (paragraphs 0042, 0043, i.e. translating the program into safe program code).

18. Regarding claims 10 and 28, Gheorghescu teaches removing said software when said software is classified as malware or unwanted software (paragraphs 0042, 0043, i.e. translating the program into safe program code).

19. Regarding claims 11 and 29, Gheorghescu teaches quarantining said software when said software is classified as malware or unwanted software (paragraph 0004).

20. Regarding claims 12 and 30, Gheorghescu teaches generating reports regarding said software (Figure 4 [step 420], paragraphs 0038, 0039).

21. Regarding claims 13 and 31, Gheorghescu teaches blocking access to said software when said software is classified as malware or unwanted software (paragraphs 0042, 0043, i.e. translating the program into safe program code).

22. Regarding claims 14 and 32, Gheorghescu teaches scanning a computer for said software, wherein said scanning include user initiated scanning, scheduled scanning and on-access scanning (Figure 4 [step 416], paragraphs 0038, 0040, i.e. identifying sections of the basic block using signatures or other characteristics of the basic block).

23. Regarding claim 15, Gheorghescu teaches wherein said classification is based upon one or more groupings of genes (Figure 4 [step 422], paragraphs 0039, 0040, i.e. classifying the basic block as being infected with malware based on the signature or other characteristics of the malware).

Art Unit: 2439

24. As per claim 16, Gheorghescu teaches a method for generating software classifications for use in classifying software, said method comprising:

identifying one or more genes that appear in software (paragraphs 0009, 0034, 0042, i.e. dividing the program code into “basic blocks,” and identifying successor and subsequent basic blocks);

combining a plurality of genes to form a set of genes (paragraph 0034, i.e. identifying successor basic blocks);

testing said set of genes for false-positives against one or more reference files (Figure 4 [steps 416, 418], paragraphs 0034, 0038, 0039, 0040, i.e. scanning those basic blocks for malware); and

defining a software classification based on said set of genes (Figure 4 [steps 420, 422], paragraphs 0039, 0040, i.e. classifying the basic block as being infected with malware based on the signature or other characteristics of the malware).

25. Regarding claim 17, Gheorghescu teaches wherein said software classification classifies malware (Figure 4 [step 422], paragraphs 0039, 0040, i.e. classifying the basic block as being infected with malware based on the signature or other characteristics of the malware).

26. Regarding claim 18, Gheorghescu teaches wherein said software classification classifies unwanted software (Figure 4 [step 422], paragraphs 0039, 0040, i.e. classifying the basic block as being infected with malware based on the signature or other characteristics of the malware).

Art Unit: 2439

27. Regarding claim 33, Gheorghescu teaches a classification generation routine configured to generate software classifications, said classification routine executing the steps of:

identifying a software functionality (paragraphs 0009, 0034, 0042);

defining a characteristic based on said identified software functionality (Figure 4 [step 416], paragraphs 0034, 0038, 0040, i.e. identifying sections of the basic block using signatures or other characteristics of the basic block); and

combining a plurality of characteristics to form a classification (Figure 4 [steps 420, 422], paragraphs 0039, 0040, i.e. classifying the basic block as being infected with malware based on the signature or other characteristics of the malware).

Conclusion

28. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

29. The following patents are cited to further show the state of the art with respect to identifying malware in program code, such as:

United States Patent Application Publication No. 2007/0240212 A1 to Matalytski, which is cited to show disassembling a program to detect malicious behavior (paragraph 0022).

United States Patent Application Publication No. 2008/0010538 A1 to Satish et al., which is cited to show detecting suspicious embedded malicious content in file formats by disassembling the data file and scanning it for malicious code.

United States Patent No. 7,636,856 B2 to Gheorghescu et al., which is cited to show the patent that issued from the published application used to reject the claims of the instant application.

Art Unit: 2439

United States Patent No. 6,357,008 B1 to Nachenberg, which is cited to show detecting malicious software heuristically after decrypting and evaluating programs.

United States Patent No. 5,826,013 A to Nachenberg, which is cited to show detecting polymorphic viruses by analyzing program code.

United States Patent No. 7,636,945 B2 to Chandnani et al., which is cited to show detecting viruses using lexical analysis.

United States Patent No. 7,519,997 B2 to Shipp, which is cited to show detecting malicious data in executable code heuristically.

United States Patent No. 7,496,963 B2 to Shipp, which is cited to show detecting malicious data in executable code heuristically.

United States Patent No. 7,069,583 B2 to Yann et al., which is cited to show detecting viruses heuristically by analyzing dataflow.

United States Patent No. 7,013,483 B2 to Cohen et al., which is cited to show emulating executable code to detect malware.

30. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian LaForgia whose telephone number is (571)272-3792.

The examiner can normally be reached on Monday thru Thursday 7-5.

31. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad can be reached on (571) 272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2439

32. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christian LaForgia/
Primary Examiner, Art Unit 2439

clf

Notice of References Cited	Application/Control No. 11/428,203		Applicant(s)/Patent Under Reexamination GODWOOD ET AL.	
	Examiner Christian LaForgia		Art Unit 2439	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-5,826,013 A	10-1998	Nachenberg, Carey S.	726/22
*	B	US-6,357,008 B1	03-2002	Nachenberg, Carey S.	726/24
*	C	US-7,013,483 B2	03-2006	Cohen et al.	726/25
*	D	US-7,069,583 B2	06-2006	Yann et al.	726/4
*	E	US-2006/0123244 A1	06-2006	Gheorghescu et al.	713/188
*	F	US-2007/0240212 A1	10-2007	Matalytski, Siarhei	726/022
*	G	US-2008/0010538 A1	01-2008	Satish et al.	714/38
*	H	US-7,496,963 B2	02-2009	Shipp, Alexander	726/24
*	I	US-7,519,997 B2	04-2009	Shipp, Alexander	726/24
*	J	US-7,636,945 B2	12-2009	Chandnani et al.	726/24
*	K	US-7,636,856 B2	12-2009	Gheorghescu et al.	713/188
	L	US-			
	M	US-			


FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS


*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

<i>Index of Claims</i> 	Application/Control No. 11428203	Applicant(s)/Patent Under Reexamination GODWOOD ET AL.
	Examiner Christian LaForgia	Art Unit 2439

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

<input type="checkbox"/> Claims renumbered in the same order as presented by applicant											<input type="checkbox"/> CPA											<input type="checkbox"/> T.D.											<input type="checkbox"/> R.1.47										
CLAIM		DATE																																									
Final	Original	05/14/2010																																									
	1	✓																																									
	2	✓																																									
	3	✓																																									
	4	✓																																									
	5	✓																																									
	6	✓																																									
	7	✓																																									
	8	✓																																									
	9	✓																																									
	10	✓																																									
	11	✓																																									
	12	✓																																									
	13	✓																																									
	14	✓																																									
	15	✓																																									
	16	✓																																									
	17	✓																																									
	18	✓																																									
	19	✓																																									
	20	✓																																									
	21	✓																																									
	22	✓																																									
	23	✓																																									
	24	✓																																									
	25	✓																																									
	26	✓																																									
	27	✓																																									
	28	✓																																									
	29	✓																																									
	30	✓																																									
	31	✓																																									
	32	✓																																									
	33	✓																																									

Search Notes 	Application/Control No. 11428203	Applicant(s)/Patent Under Reexamination GODWOOD ET AL.
	Examiner Christian LaForgia	Art Unit 2439

SEARCHED			
Class	Subclass	Date	Examiner
none	none	5/13/10	clf

SEARCH NOTES		
Search Notes	Date	Examiner
EAST search - see enclosed	5/13/10	clf
IEEE search	5/13/10	clf
ACM search	5/13/10	clf
Google search	5/13/10	clf
Inventor search	5/13/10	clf
Assignee search	5/13/10	clf

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

	/Christian LaForgia/ Primary Examiner.Art Unit 2439
--	--



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
 United States Patent and Trademark Office
 Address: COMMISSIONER FOR PATENTS
 P.O. Box 1450
 Alexandria, Virginia 22313-1450
 www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 3669

SERIAL NUMBER 11/428,203	FILING or 371(c) DATE 06/30/2006 RULE	CLASS 726	GROUP ART UNIT 2439	ATTORNEY DOCKET NO. SPHS-0007-P01		
APPLICANTS Ben Godwood, Finstock, UNITED KINGDOM; William James McCourt, Abingdon, UNITED KINGDOM; ** CONTINUING DATA ***** ** FOREIGN APPLICATIONS ***** ** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ** 07/25/2006						
Foreign Priority claimed <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No 35 USC 119(a-d) conditions met <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No Verified and /CHRISTIAN A LAFORGIA/ Acknowledged Examiner's Signature		<input type="checkbox"/> Met after Allowance Initials	STATE OR COUNTRY UNITED KINGDOM	SHEETS DRAWINGS 3	TOTAL CLAIMS 33	INDEPENDENT CLAIMS 3
ADDRESS STRATEGIC PATENTS P.C.. C/O PORTFOLIOIP P.O. BOX 52050 MINNEAPOLIS, MN 55402 UNITED STATES						
TITLE METHOD AND SYSTEM FOR CLASSIFICATION OF SOFTWARE USING CHARACTERISTICS AND COMBINATIONS OF SUCH CHARACTERISTICS						
FILING FEE RECEIVED 1780	FEES: Authority has been given in Paper No. _____ to charge/credit DEPOSIT ACCOUNT No. _____ for following:		<input type="checkbox"/> All Fees <input type="checkbox"/> 1.16 Fees (Filing) <input type="checkbox"/> 1.17 Fees (Processing Ext. of time) <input type="checkbox"/> 1.18 Fees (Issue) <input type="checkbox"/> Other _____ <input type="checkbox"/> Credit			

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	1	(US-20060123244-\$).did.	US-PGPUB	OR	OFF	2010/05/13 12:22
L2	1	1 and quarantin\$3	US-PGPUB; USPAT	OR	ON	2010/05/13 12:22
S1	3	sophos.as.	US-PGPUB; USPAT	OR	ON	2010/05/13 09:11
S2	3	godwood-ben\$.in.	US-PGPUB; USPAT	OR	ON	2010/05/13 09:11
S3	4	mccourt-william\$.in.	US-PGPUB; USPAT	OR	ON	2010/05/13 09:14
S4	2	("20050172338" "20040181677").pn.	US-PGPUB; USPAT	OR	ON	2010/05/13 09:16
S5	5	("2005/0172338").URPN.	USPAT	OR	OFF	2010/05/13 09:21
S6	0	("2004/0181677").URPN.	USPAT	OR	OFF	2010/05/13 09:22
S7	0	("2004/0181677").URPN.	USPAT	OR	OFF	2010/05/13 09:22
S8	1	(anti\$virus (malware virus trojan adware spyware dialer) near detect\$3) same (detect\$3 determin\$5) with (malware malicious trojan adware spyware dialer) with (decompil\$3 disassembl\$3) with (program code)	US-PGPUB; USPAT	OR	ON	2010/05/13 09:25
S9	8	(detect\$3 determin\$5) with (malware malicious trojan adware spyware dialer) with (decompil\$3 disassembl\$3) with (program code)	US-PGPUB; USPAT	OR	ON	2010/05/13 09:27

S10	63	(detect\$3 determin\$5) with (malware malicious trojan adware spyware dialer) with (characteristic) with (program code)	US-PGPUB; USPAT	OR	ON	2010/05/13 09:30
S11	8	(detect\$3 determin\$5) with (malware malicious trojan adware spyware dialer) with (characteristic) with (program code) and (disassembl\$3 unpack\$3)	US-PGPUB; USPAT	OR	ON	2010/05/13 09:31
S13	3	("2006/0123244").URPN.	USPAT	OR	OFF	2010/05/13 11:20
S14	11	((("20050005153") or ("20040041315") or ("5381533") or ("5765030") or ("20020091934") or ("6704925") or ("5826013") or ("5951698") or ("6357008") or ("20030101381") or ("6637514")).PN.	US-PGPUB; USPAT	OR	OFF	2010/05/13 11:28
S15	77	("6357008").URPN.	USPAT	OR	OFF	2010/05/13 11:30
S16	74	("5826013").URPN.	USPAT	OR	OFF	2010/05/13 11:38

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S12	1	sophos.as.	USPAT; UPAD	OR	ON	2010/05/13 09:11

5/ 13/ 10 1:21:23 PM**C:\ Documents and Settings\ claforgia\ My Documents\ EAST\ Workspaces\ 11428203.wsp**

Substitute for form 1449A/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Complete if Known</i> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 40%;">Application Number</td> <td>11/428,203</td> </tr> <tr> <td>Filing Date</td> <td>June 30, 2006</td> </tr> <tr> <td>First Named Inventor</td> <td>Godwood, Ben</td> </tr> <tr> <td>Art Unit</td> <td>Unknown</td> </tr> <tr> <td>Examiner Name</td> <td>Unknown</td> </tr> </table>		Application Number	11/428,203	Filing Date	June 30, 2006	First Named Inventor	Godwood, Ben	Art Unit	Unknown	Examiner Name	Unknown
Application Number	11/428,203														
Filing Date	June 30, 2006														
First Named Inventor	Godwood, Ben														
Art Unit	Unknown														
Examiner Name	Unknown														
Sheet	1	of	1	Attorney Docket No: SPHS-0007-P01											

US PATENT DOCUMENTS					
Examiner Initial *	Cite No	Document Number	Publication Date	Name of Patentee or Applicant of Cited Document	Filing Date If Appropriate
/CLF/		US-20050172338	08/04/2005	Sandu, Catalin D., et al.	01/30/2004
/CLF/		US-20040181677	08/16/2004	Man-Pyo, Hong et al.	10/30/2003

FOREIGN PATENT DOCUMENTS					
Examiner Initials*	Cite No	Foreign Patent Document	Publication Date	Name of Patentee or Applicant of cited Document	T ²
/CLF/	A	IB-WO2006006144	01/19/2006	Zamir, Shay , et al.	

OTHER DOCUMENTS -- NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T ²
/CLF/	B	"Search Report Under Section 17(5)", <u>For Application No. GB0711866.4, mailed October 12, 2007.</u>	

EXAMINER

/Christian LaForgia/

DATE CONSIDERED

05/13/2010



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
11/428,203	06/30/2006	Ben Godwood	SPHS-0007-P01

CONFIRMATION NO. 3669

POA ACCEPTANCE LETTER

43520
STRATEGIC PATENTS P.C..
C/O PORTFOLIOIP
P.O. BOX 52050
MINNEAPOLIS, MN 55402



Date Mailed: 06/26/2008

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 06/18/2008.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

/mtekle michael/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
11/428,203	06/30/2006	Ben Godwood	17678US01

CONFIRMATION NO. 3669

POWER OF ATTORNEY NOTICE



OC000000030662911

23446
MCANDREWS HELD & MALLOY, LTD
500 WEST MADISON STREET
SUITE 3400
CHICAGO, IL 60661

Date Mailed: 06/26/2008

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 06/18/2008.

- The Power of Attorney to you in this application has been revoked by the assignee who has intervened as provided by 37 CFR 3.71. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

/mtekle michael/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

RECEIVED
CENTRAL FAX CENTER
JUN 18 2008



Fax

To:	Commissioner for Patents	From:	Robert A. Mazzaresse
Fax:	(571)273-8300	Fax:	(781) 644-6137
Phone:		Phone:	(781) 453-9993
<hr/>			
Date:	6/18/2008		
Subject:	Revocation and New Power of Attorney		

Comments

Inventor:	Godwood, Benjamin John
Serial No:	11/428,203
Filed:	June 30, 2006
For:	METHOD AND SYSTEM FOR CLASSIFICATION OF SOFTWARE USING CHARACTERISTICS AND COMBINATIONS OF SUCH CHARACTERISTICS
Examiner:	N/A
Art Unit:	3669

Strategic Patents, P.C. | P.O. Box 920629 | Needham, MA 02492 | United States
phone: (781) 453-9993 | eFax: (781) 644-6137
www.strategic-patents.com

Docket No.: SPHS-0007-P01

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor: Godwood, Benjamin John
Serial No: 11/428,203
Filed: June 30, 2006
For: METHOD AND SYSTEM FOR CLASSIFICATION OF
SOFTWARE USING CHARACTERISTICS AND
COMBINATIONS OF SUCH CHARACTERISTICS
Examiner: N/A
Art Unit: 3669

RECEIVED
CENTRAL FAX CENTER
JUN 18 2008

CERTIFICATE OF FACSIMILE TRANSMISSION UNDER 37 C.F.R. §1.8(a)

The undersigned hereby certifies that this document is transmitted via facsimile to the
Commissioner for patents at (571) 273-8300 on June 18, 2008.

/Robert Mazzaresse/

Robert A. Mazzaresse

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Transmitted herewith is a Revocation and New Power of Attorney for entry into the
above case. Pursuant to attached document, kindly take the following actions:

1. Revoke any existing powers of attorney, and appoint **all practitioners associated with PTO Customer No. 43520** to prosecute this application, and to transact all business in the Patent and Trademark Office in Connection therewith. The fee address should not be changed.
2. Direct all correspondence in this case to **Customer No. 43520**.
3. Change the attorney docket number in these case to **SPHS-0007-P01**

Please contact the undersigned if there are any questions relating to this submission.

Respectfully submitted,

Strategic Patents, P.C.

By: 

Robert A. Mazzaresse
Reg. No. 42,852
(781) 453-9993

Date: June 18, 2008

RECEIVED
CENTRAL FAX CENTER
JUN 18 2008

REVOCATION AND POWER OF ATTORNEY
For SOPHOS PLC

Page 1 of 3

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

REVOCATION AND NEW POWER OF ATTORNEY
and
CERTIFICATE UNDER 37 CFR § 3.73(b)
and
CHANGE OF CORRESPONDENCE ADDRESS
and
REQUEST TO CHANGE ATTORNEY DOCKET NUMBER

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REVOCATION AND NEW POWER OF ATTORNEY

In accordance with 37 C.F.R. Section 1.36, M.P.T.P. Section 402.05 and 402.07, please revoke any existing Powers of Attorney and appoint the following attorneys and/or patent agents to prosecute the applications identified in Appendix A hereto, and to transact all business in the Patent and Trademark Office in connection therewith:

All practitioners associated with PTO Customer No. 43520

CERTIFICATE UNDER 37 CFR § 3.73(b)

Sophos PLC hereby certifies that it is the assignee of the entire right, title and interest in the patent applications identified in Appendix A by virtue of assignments from the previous owner(s). Appendix A includes a reel and frame number for the assignment(s) of each application identified therein. To the best of my knowledge and belief, title is in Sophos PLC, the assignee.

Pursuant to 37 C.F.R. § 3.73(b) I hereby declare that I, PAUL SMOLINSKI, am empowered to sign this certificate on behalf of Sophos PLC, the assignee.

REVOCATION AND POWER OF ATTORNEY
For SOPHOS PLC

Page 2 of 3

CHANGE OF CORRESPONDENCE ADDRESS

Please direct all correspondence in the applications and patents identified in Appendix A to:

Customer No. 43520

REQUEST TO CHANGE ATTORNEY DOCKET NUMBER

Please change the attorney docket number associated with the each of the patents and applications identified in Appendix A to the number listed under the heading, "New Atty. No."

I hereby declare that all statement made herein of my own knowledge are true, and that all statements made on information and belief are believed to be true.

Date 5 June 2008

By



PAUL SOKOLINSKI (Printed Name)

C.F.O. (Title)

Sophos PLC

REVOCATION AND POWER OF ATTORNEY
For SOPHOS PLC

Page 3 of 3

Appendix A
Listing of Patents and Pending Applications

Serial No.	TITLE	New App. No.	Filing Date	Comments	Ass'n Reel	Age'n Frame
10/747,381	METHOD AND SYSTEM FOR FEATURE EXTRACTION FROM OUTGOING MESSAGES FOR USE IN CATEGORIZATION OF INCOMING MESSAGES	SPHS-0005- P01	29-Dec-03	From Inventors to Activestate Co.	014859	0106
10/747,381	METHOD AND APPARATUS FOR FILTERING ELECTRONIC MAIL	SPHS-0005- P01	29-Dec-03	From Activestate Co. to Sophos PLC	020918	0499
11/428,203	METHOD AND SYSTEM FOR CLASSIFICATION OF SOFTWARE USING CHARACTERISTICS AND COMBINATIONS OF SUCH CHARACTERISTICS	SPHS-0007- P01	30-Jun-04	From inventors to Sophos PLC	018085	0141
11/676,754	METHOD AND SYSTEM FOR UNSAFE CONTENT TRACKING	SPHS-0008- P01	20-Feb-07	From Inventors to Sophos PLC	018909	0021
11/688,930	SYSTEMS AND METHODS FOR DYNAMIC VENDOR AND VENDOR OUTLET CLASSIFICATION	SPHS-0009- P01	22-Mar-07	From inventors to Sophos PLC	020979	0457
11/690,477	PRE-FETCHING WEB PROXY	SPHS-0010- P01	23-Mar-07	From inventors to Sophos PLC	019059	0021

Substitute for form 1449A/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				<i>Complete if Known</i>	
				Application Number	11/428,203
				Filing Date	June 30, 2006
				First Named Inventor	Godwood, Ben
				Art Unit	Unknown
				Examiner Name	Unknown
Sheet	1	of	1	Attorney Docket No: SPHS-0007-P01	

US PATENT DOCUMENTS					
Examiner Initial *	Cite No	Document Number	Publication Date	Name of Patentee or Applicant of Cited Document	Filing Date If Appropriate
		US-20050172338	08/04/2005	Sandu, Catalin D., et al.	01/30/2004
		US-20040181677	08/16/2004	Man-Pyo, Hong et al.	10/30/2003

FOREIGN PATENT DOCUMENTS					
Examiner Initials*	Cite No	Foreign Patent Document	Publication Date	Name of Patentee or Applicant of cited Document	T ²
	A	IB-WO2006006144	01/19/2006	Zamir, Shay , et al.	

OTHER DOCUMENTS -- NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T ²
	B	"Search Report Under Section 17(5)", <u>For Application No. GB0711866.4, mailed October 12, 2007.</u>	

EXAMINER

DATE CONSIDERED

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Ben Godwood et al.	Examiner:	Unknown
Serial No.:	11/428,203	Group Art Unit:	Unknown
Filed:	June 30, 2006	Docket:	SPHS-0007-P01
Title:	METHOD AND SYSTEM FOR CLASSIFICATION OF SOFTWARE USING CHARACTERISTICS AND COMBINATIONS OF SUCH CHARACTERISTICS		

INFORMATION DISCLOSURE STATEMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

In compliance with the duty imposed by 37 C.F.R. § 1.56, and in accordance with 37 C.F.R. §§ 1.97 *et. seq.*, the referenced materials are brought to the attention of the Examiner for consideration in connection with the above-identified patent application. Applicants respectfully request that this Information Disclosure Statement be entered and the documents listed on the attached Form 1449 be considered by the Examiner and made of record. Pursuant to the provisions of MPEP 609, Applicants request that a copy of the 1449 form, initialed as being considered by the Examiner, be returned to the Applicants with the next official communication.

Pursuant to 37 C.F.R. §1.97(b), it is believed that no fee or statement is required with the Information Disclosure Statement. However, if an Office Action on the merits has been mailed, the Commissioner is hereby authorized to charge the required fees to Deposit Account No. 50-4262 in order to have this Information Disclosure Statement considered. The Examiner is invited to contact the Applicants' Representative at the below-listed telephone number if there are any questions regarding this communication.

INFORMATION DISCLOSURE STATEMENT

Serial No :11/428,203

Filing Date: June 30, 2006

Title: METHOD AND SYSTEM FOR CLASSIFICATION OF SOFTWARE USING CHARACTERISTICS AND COMBINATIONS OF SUCH CHARACTERISTICS

Page 2

Dkt: SPHS-0007-P01

Pursuant to 37 C.F.R. 1.98(a)(2), Applicant believes that copies of cited U.S. Patents and Published Applications are no longer required to be provided to the Office. Notification of this change was provided in the United States Patent and Trademark Office OG Notices dated October 12, 2004. Thus, Applicant has not included copies of any US Patents or Published Applications cited with this submission. Should the Office require copies to be provided, Applicant respectfully requests that notice of such requirement be directed to Applicant's below-signed representative. Applicant acknowledges the requirement to submit copies of foreign patent documents and non-patent literature in accordance with 37 C.F.R. 1.98(a)(2).

Respectfully submitted,

STRATEGIC PATENTS, P.C.

Date January 5, 2008

By /Robert Mazzaresse/
Robert A. Mazzaresse
Reg. No. 42,852
Customer No. 43520
781-453-9993

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
19 January 2006 (19.01.2006)

PCT

(10) International Publication Number
WO 2006/006144 A2

(51) International Patent Classification:
G06F 11/00 (2006.01)

(21) International Application Number:
PCT/IL2005/000648

(22) International Filing Date: 16 June 2005 (16.06.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/890,170 14 July 2004 (14.07.2004) US

(71) Applicant: **Aladdin Knowledge Systems Ltd.** [IL/IL];
15 Beit Oved St., 61110 Tel Aviv (IL).

(72) Inventors: **ZAMIR, Shay**; 33 Hatapuz St., 36848 Neshet
(IL). **MARGALIT, Yanki**; 6 Carmeli St, Ramat Gan (IL).
MARGALIT, Dany; 5 Yair St., 52238 Ramat Gan (IL).

(81) Designated States (unless otherwise indicated, for every
kind of national protection available): AE, AG, AL, AM,

AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN,
CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI,
GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE,
KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA,
MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ,
OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL,
SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN,
YU, ZA, ZM, ZW.

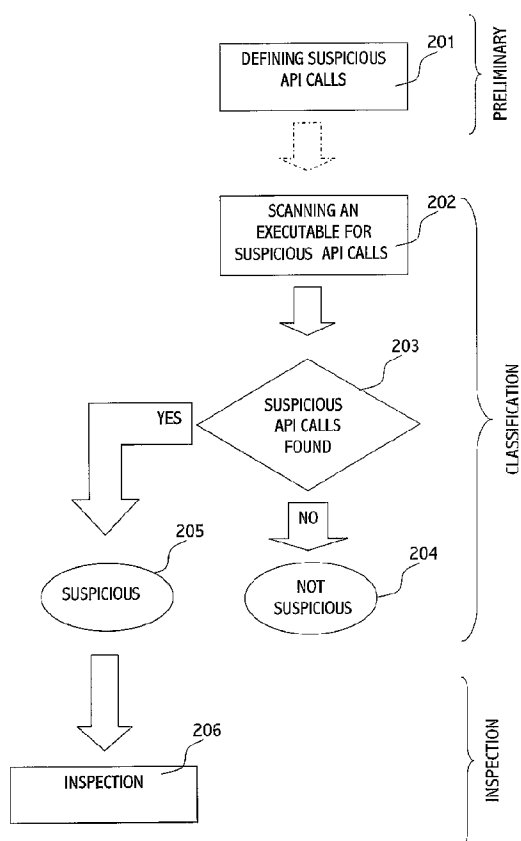
(84) Designated States (unless otherwise indicated, for every
kind of regional protection available): ARIPO (BW, GH,
GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM,
ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),
European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI,
FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO,
SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN,
GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— without international search report and to be republished
upon receipt of that report

For two-letter codes and other abbreviations, refer to the "Guide-
ance Notes on Codes and Abbreviations" appearing at the begin-
ning of each regular issue of the PCT Gazette.

(54) Title: A METHOD FOR DETECTING OF UNWANTED EXECUTABLES



(57) Abstract: The present invention is directed to a method for detecting unwanted executables and preventing the damage thereof, comprising: defining at least one API call as suspicious; scanning an executable for detecting suspicious API calls; and upon detecting a suspicious API call within said executable, either just determining said executable as unwanted or inspecting said executable. Following inspection, if said executable is indicated as unwanted and/or malicious, the damage thereof is prevented by eliminating the suspicious calls from said executable, discarding said executable, etc.

A METHOD FOR DETECTING UNWANTED EXECUTABLESField of the Invention

5 The present invention relates to the field of detecting unwanted computer executables.

Background of the Invention

10 As the Internet becomes a major communication channel, it has also turned to be a channel for propagating "annoying" content. One of the known forms of annoying content is Spam, i.e. email messages that reach a user's email box, and usually contain advertising
15 content.

 The recent forms of annoying content are the adware, which cause advertising content to pop-up on the user's display while browsing the Internet, and the spyware,
20 which tracks the browsing habits of a user and reports it to a remote site, in order to focus the content of advertising material, or even worse, to collect confidential information of a user.

In order to facilitate the reading of the description to follow, the following terms and acronyms are explained:

- 5 The term "unwanted content" refers herein to content that a user may be exposed to, against his will. Annoying content is an example of unwanted content.

10 The term "unwanted executable" refers herein to an executable (program, script, etc.) that causes exposure of a user to unwanted content, whether directly (e.g. by displaying unwanted content) or indirectly (e.g. by changing the default home page address of a browser).

- 15 There are a variety of ways to propagate unwanted objects (content and/or executables). For example, while browsing the Internet, a user's computer is exposed to installation of unwanted objects, even without the user being aware of it. Moreover, installation of unwanted
20 objects within a user's computer may be carried out by his acceptance and collaboration. For example, a user that installs on his computer a shareware or freeware program usually selects the defaults of the installation, especially if he is not a computer specialist. During the
25 installation he may be asked if he would like to receive further information, and since he usually selects the

default option, an adware program can be installed on his computer.

There are a variety of means that cause displaying
5 of unwanted content. For example, programs that are
executed when the operating system starts up can be used
for this purpose; the default homepage of a Web browser
can be used as a means for indirectly displaying unwanted
content; a browser toolbar can also be used for
10 displaying unwanted content; an installation procedure
can also be used for installing unwanted executables; and
many other ways.

Usually unwanted objects cannot be considered as
15 "viral", since they do not multiply themselves, and also
do not harm the user's computer. Consequently the known
methods of detecting viral presence, such as virus
signatures, may be less effective for detecting unwanted
objects.

20

It is an object of the present invention to provide
a method for detecting unwanted executables.

It is another object of the present invention to
25 provide a method for detecting unwanted executables, in

which the detection can be carried out in a virtual platform.

It is a further object of the present invention to
5 provide a method for detecting unwanted executables, by
which spyware, adware, operating system startup
executables, and so forth can be detected.

Other objects and advantages of the invention will
10 become apparent as the description proceeds.

Summary of the Invention

In one aspect, the present invention is directed to a method for detecting unwanted executables (e.g. spyware, adware, viral executable, malicious executable, etc.), the method comprising the steps of:

- defining at least one API call as suspicious;
 - scanning an executable for detecting suspicious API calls; and
- 10- upon detecting a suspicious API call within the executable, determining the executable as an unwanted executable.

The suspicious API call may refer to a certain API function, a certain parameter of an API function, and a certain API function with at least a certain parameter.

The API function may have relevance to registry access, registry update, startup of an operating system, homepage of a Web browser, dialing, communication, file system, Internet browser, user interface, and so forth.

The scanning may be carried out on a real platform or a virtual platform.

The method may further comprise sterilizing the executable and/or discarding the executable.

In another aspect, the present invention is directed
5 to a method for detecting unwanted executables (e.g. spyware, adware, dialer, key logger, listener, viral executable, malicious executable, etc.) and preventing the damage thereof, the method comprising the steps of:

- defining at least one API call as suspicious;
- 10 - scanning an executable for detecting suspicious API calls; and
- upon detecting a suspicious API call within the executable, inspecting the executable.

15 The suspicious API call may be a certain API function, at least a certain parameter of an API function, and a certain API function with at least a certain parameter.

20 The API function has relevance to a member of a group comprising: a registry access, a registry update, startup of an operating system, homepage of a Web browser, dialing, communication, file system, Internet browser, user interface, and so forth.

The scanning may be carried out on a real platform or a virtual platform.

The executable may be a readable object, a compiled
5 object, etc.

Inspecting may be carried out in order to indicate if the executable is malicious and/or unwanted.

10 The method may further comprise: upon indicating the executable as unwanted and/or malicious, discarding the executable.

The method may further comprise: upon indicating the
15 executable as unwanted and/or malicious, sterilizing or discarding the executable.

Brief Description of the Drawings

The present invention may be better understood in conjunction with the following figures:

5

Fig. 1 schematically illustrates a system that may be used for implementing the present invention.

Fig. 2 is a flowchart of a process for detecting
10 unwanted executables, according to a preferred embodiment of the invention.

Fig. 3 is a flowchart of a process for detecting
unwanted executables, according to another preferred
15 embodiment of the present invention.

Detailed Description of Preferred Embodiments

In the art, the term gateway refers to a network point that acts as an entrance to another network. As
5 such, a gateway is a suitable point for filtering unwanted objects.

A system that provides the connectivity between the two networks is referred in the art as a gateway server.
10 From the implemental point of view, a gateway server is often associated with both a router, which knows where to direct a given packet of data that arrives at the gateway and a switch, which furnishes the actual path in and out of the gateway for a given packet. The connectivity can
15 be carried out at any level of the OSI model, from application protocols to low-level signaling. Because a gateway by definition appears at the edge of a network, related functionality like fire-walling tends to exist at the same location.

20

Fig. 1 schematically illustrates a system that may be used for implementing the present invention. The computers 21 are connected to the local area network 20. The local area network 20 is connected to the Internet
25 10. The gateway server 30 is interposed between the local area network 20 and the internet 10. The internet server

40 hosts Web sites. A browser being executed on a computer 21 that addresses the Web site hosted by the Internet server 40 cause files to be transferred from the Internet server 40 to the computer 21 through the gateway
5 server 30. The transferred file can be inspected on a real platform, i.e. on the user's computer, or on the virtual platform, e.g. the gateway server 30.

In terms of real / virtual platforms, the computer
10 21 is a real platform, and the gateway server 30 may be implemented as a virtual platform.

The conditions of inspecting executables on a virtual platform are substantially different than the
15 conditions of inspecting executables on a real platform. Firstly, a virtual platform has to deal with a great amount of executables that passes through it at any given moment, contrary to a real platform which deals with individual executables. Also it is not practical to
20 execute each suspicious executable on a virtual platform, in order to track its behavior. Moreover, executables may be designed to interact with a user, and it is not practical to employ a human factor on a virtual platform to interact with every suspicious executable.

As such, the methods for inspecting executables on a gateway usually differ from the methods used for inspecting executables on a personal computer.

5 Inspection, i.e. detection of unwanted and malicious objects, is usually carried out on one of two platforms:

- (a) on a real platform, i.e. on the user's computer; and
- (b) on a virtual platform, i.e. any computer but not the user's computer, in order to prevent possible damage to

10 the user's computer. A real platform provides more possibilities to monitor the executable, thereby to detect unwanted objects, but a virtual platform provides a shield, since unwanted objects can be stopped before reaching a user's computer.

15

 The term API (Application Program Interface) refers in the art to a set of routines, protocols, and tools (referred herein also as API functions) for causing a first program to be operated by another program.

20 Consequently the first program can be treated as a "black-box" which interacts with the outside world by API functions. For example, operating system services can be activated by application programs via dedicated API functions.

25

The term API call refers herein to code for invoking an API function, parameter(s) of an API function, code for invoking an API function with certain parameter(s), etc.

5

Dialer is a common nickname for a program which reroutes a user's Internet connection through a high paid telephone number. A user that connects to the Internet through a dial-up connection may be rerouted by a Dialer to a high paid number instead of his regular connection, and consequently his telephone account gets charged for telephone calls that he has not intended to do, usually at a high cost. From the technical point of view, under the Windows operating system, a Dialer uses API calls of the MODEM API module. Thus, an executable program may be classified as suspicious if it calls to certain MODEM API functions. Moreover, an executable program can be identified as Dialer by the existence of a combination of a certain MODEM API call with a known high paid telephone number as parameter.

Key loggers are programs that record a list of key strokes carried out by a user while typing, and send it via the Internet to a hostile object. The list of key strokes (known as log) can be used for detecting passwords, credit card numbers etc. From the technical

25

point of view, key loggers use a certain type of API, which is known as "Hooking API". Thus, a program that uses function of the Hooking API is suspicious, especially if the call is with certain value of its
5 parameters.

"Listeners" are programs that open a back door" to the user s computer by listening to some TCP/IP port. Listeners can be detected by looking for a certain API
10 usage of the windows socket API. Such a use of API calls can be carried out also due to a legitimate reason. Thus, it is up to the user or network administrator to decide whether such a use is valid for a certain program.

15 Fig. 2 is a flowchart of a process for detecting unwanted executables, according to a preferred embodiment of the present invention.

The process is divided into two parts: a preliminary
20 stage, and a run time stage. In the preliminary stage, at block 101, a group of suspicious API calls is defined. A definition of a suspicious API call can be a call to a specific API function, a call to any API function with specific parameter(s), a combination of both, i.e. a call
25 to a specific API function with specific parameter(s), and so forth.

In run time, at block 102, when an executable reaches the gateway, it is scanned for API calls, and those API calls found are compared against the list of suspicious API calls. From block 103, if a suspicious API call has been found in the executable, then the executable is considered to be suspicious, as indicated in block 105, otherwise the executable may be considered as unsuspicious, as indicated by block 104.

10

Fig. 3 is a flowchart of a process for detecting unwanted executables, according to another preferred embodiment of the present invention.

15

The process is divided into three parts:

- A preliminary stage, in which a group of API functions are determined as suspicious: At block 201, a group of suspicious API calls is defined. A definition of a suspicious API call can be a call to a specific API function, a call to any API function with specific parameter(s), a combination of both, i.e. a call to a specific API function with specific parameter(s), and so forth.

25

- A classification stage, in which an executable is classified as suspicious or unsuspicious: At block 202, when an executable reaches the gateway, it is scanned for API calls, and the found API calls are compared against the list of suspicious API calls. From block 203, if a suspicious API call has been found in the executable, then the executable is considered to be suspicious, as indicated in block 205, otherwise the executable may be considered as unsuspicious, as indicated by block 204.
- An inspection stage, in which a suspicious executable is further inspected for classifying the executable as unwanted and/or malicious, as indicated in block 206.

The classification stage is used for classifying an executable as suspicious or unsuspicious, and the inspection stage is used for inspecting a suspicious executable, usually by more intensive inspection tests.

In other words, in the classification stage, a rough estimation of the possibility of existence of suspicious calls can be indicated, in order to decide if the inspected executable should be further inspected by more intensive tests. The inspection stage according to its

nature may be slower than the first inspection stage however it can be more effective. Furthermore, the intensive inspection can be used for detecting other forms of unwanted content.

5

Detecting API calls within an executable such as Windows EXE and JAVA can be carried out, for example, by a simulation engine. In this method, the execution code is scanned, and the simulation engine performs the
10 actions set by the scanned code on its internal data, simulating the operation of the CPU and the operating system. When the executed code performs a call to an outside DLL or COM object, the function name and parameters are compared to a known set of suspicious
15 functions and parameters upon which the code is indicated as suspicious or unsuspicious.

Another method for detecting function calls is by disassembly. In this case, code bytes are scanned,
20 identified and translated into code lines. The code lines are analyzed in order to detect patterns of API calls. Found API calls are cross referenced into actual API destinations. According to this method, no execution or simulation is required, and therefore it is faster than a
25 simulation method. This method is not effective for

detecting encrypted parameter values or dynamically created parameters.

In the Microsoft Windows operating systems, a
5 registry is a database that stores information about the configuration of the operating system, installed applications, attached hardware, optional components such as ODBC, what system options have been selected, how the computer memory is set up, what application programs are
10 to be present when the operating system starts, the association between a file extension and applications, and so forth.

The registry is somewhat similar to and a
15 replacement for the INI files and configuration files used in earlier Windows systems and DOS-based systems. INI files are still supported by the recent versions of Windows, however, usually for compatibility with 16-bit applications written for earlier systems.

20

Calling registry related functions is very common and by itself does not denote malicious intent. On the other hand, a combination of a call to a registry related function with certain parameters (such as an attempt to
25 write into a registry entry that specifies the programs

that run during booting the computer) may indicate maliciousness.

The following functions are examples of Windows API
5 functions for accessing the registry of a computer:

- **RegReplaceKey (hKey, sSubKey, sNewFile, sOldFile)**

Which allows replacing an entire hive when the system
is next booted.

10

- **RegRestoreKey (hKey, sFileName, uFlags)** Which reads
in a hive file and copies its content over an existing
registry tree.

15 For example, RegCreateKey and RegReplaceKey may
appear in several variations. They also can be called by
their ordinal number. A simulation can detect a call to
these functions and the parameter values used for the
call. The use of a registry is very common in Windows
20 applications and does not denote a malicious intent by
itself, but in combination with certain parameter values
supplied by a calling process. For example, an attempt to
replace the content of a registry entry that specifies
the programs executed during the boot procedure can turn
25 a red light on . According to one embodiment of the
invention, if this call is carried out with a parameter

that comprises a known malicious program name or URL, the executable can be classified as malicious, and the damage thereof can be prevented.

5 Typically, unwanted executables, such as spyware and
adware, use the registry for retrieving information about
the user's computer, which programs are executed at a
given moment, which Web sites have been browsed recently,
and so forth. Based on such information, an adware
10 application may pop-up a window with certain advertising
content, and a spyware application can retrieve sensitive
information such as credit card numbers, and send it to a
hostile object.

15 The Internet Explorer browser, manufactured by
Microsoft, also provides an API, upon which the way the
browser operates can be directed. For example, it is
possible to instruct the browser to open a new window for
a certain URL (Uniform Resource Location, i.e. an address
20 that defines the route to a file on the Web or any other
Internet facility). Thus, if an executable comprises a
call to an API function that opens a new window of a
known advertising URL, then the program can be classified
as adware.

According to one embodiment of the invention, a suspicious executable is discarded. According to another embodiment of the invention the code of the executable is amended such that the suspicious API calls are removed or
5 bypassed ("sterilized").

The discussion herein is directed mainly to executable code which usually cannot be detected by virus detection methods, such as virus signatures. However it
10 should be noted that the disclosed method can also be implemented with any form of executable, regardless to their object, including malicious executables. Thus, although the term unwanted executable was defined above by its object (preventing exposure of a user to unwanted
15 content), it should be noted that the disclosed method may be implemented for any executable regardless of its object.

It should be noted that although the reference and
20 examples herein refer to a registry, the term registry is directed also to other forms of databases for this purpose, such as INI files.

It should also be noted that an executable may be
25 either a compiled object (e.g. Windows EXE) or a readable object (e.g. JavaScript).

Those skilled in the art will appreciate that the invention can be embodied by other forms and ways, without losing the scope of the invention. The
5 embodiments described herein should be considered as illustrative and not restrictive.

CLAIMS

1. A method for detecting unwanted executables, the method comprising the steps of:
 - 5 - defining at least one API call as suspicious;
 - scanning an executable for detecting one of said at least one suspicious API call; and
 - upon detecting said one suspicious API call within said executable, determining said executable as unwanted10 executable.
2. A method according to claim 1, wherein said at least one suspicious API call is selected from the group comprising: a call of a certain API function, a call of
15 an API function that includes at least one certain parameter, and a call of a certain API function with at least one certain parameter.
3. A method according to claim 2, wherein said at least
20 one API function has relevance to a member of a the group comprising: a registry access, a registry update, a startup of an operating system, homepage of a Web browser, dialing, communication, a FAT, an Internet browser, a user interface.

4. A method according to claim 1, wherein said scanning is carried out on a real platform.
5. A method according to claim 1, wherein said scanning is carried out on a virtual platform.
6. A method according to claim 1, wherein said unwanted executable is selected from the group comprising:
spyware, adware, a dialer, a key logger, a listener, a
10 viral executable, a malicious executable.
7. A method according to claim 1, wherein said executable is selected from the group comprising: a readable object, a compiled object.
15
8. A method according to claim 1, further comprising the step of sterilizing said executable
9. A method according to claim 1, further comprising the
20 step of discarding said executable.
10. A method for detecting unwanted executables and preventing the damage thereof, the method comprising the steps of:
25 - defining at least one API call as suspicious;

- scanning an executable for detecting one of said at least one suspicious API call; and
- upon detecting said one suspicious API call within said executable, inspecting said executable.

5

11. A method according to claim 10, wherein said at least one suspicious API call is selected from the group comprising: a call of a certain API function, a call of an API function that includes at least one certain
10 parameter, and a call of a certain API function with at least one certain parameter.
12. A method according to claim 11, wherein said API function has relevance to a member of a group comprising:
15 a registry access, a registry update, startup of an operating system, homepage of a Web browser, dialing, communication, FAT, Internet browser, user interface.
13. A method according to claim 10, wherein said scanning
20 is carried out on a real platform.
14. A method according to claim 8, wherein said scanning is carried out on a virtual platform.
- 25 15. A method according to claim 10, wherein said unwanted executable is selected from the group comprising:

spyware, adware, a dialer, a key logger, a listener, a viral executable, a malicious executable.

16. A method according to claim 10, wherein said executable
5 is selected from the group comprising: a readable object, a compiled object.

17. A method according to claim 10, further comprising the step of sterilizing said executable.

10

18. A method according to claim 10, wherein said inspecting is carried out for indicating if said executable is malicious.

15 19. A method according to claim 10, wherein said inspecting is carried out for indicating if said executable is unwanted.

20. A method according to claim 10, further comprising the
20 step of: upon indicating said executable as unwanted, discarding said executable.

21. A method according to claim 10, further comprising the
step of: upon indicating said executable as malicious,
25 discarding said executable.

22. A method according to claim 10, further comprising the step of: upon indicating said executable as unwanted, sterilizing or discarding said executable.
523. A method according to claim 10, further comprising the step of: upon indicating said executable as malicious, sterilizing or discarding said executable.

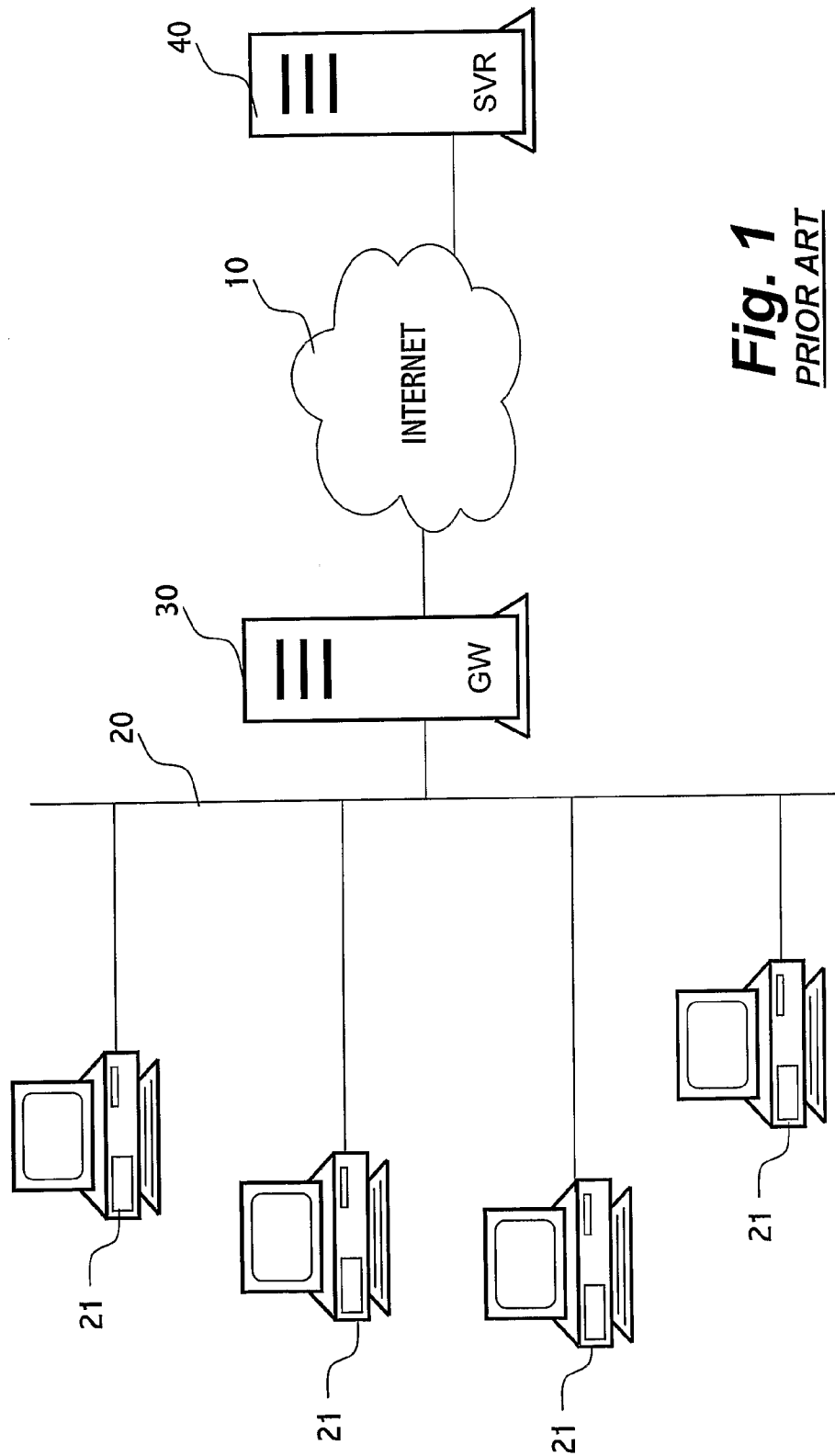
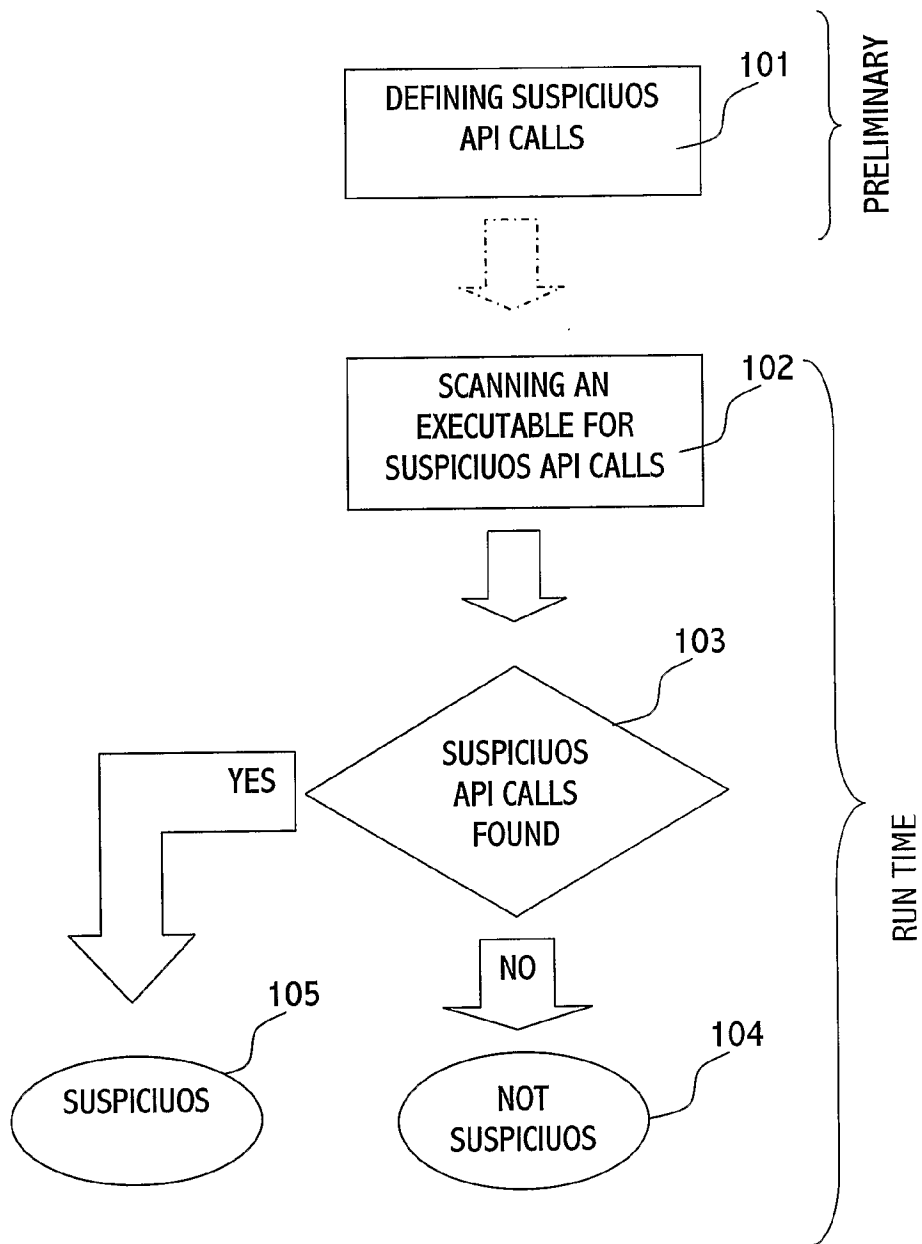
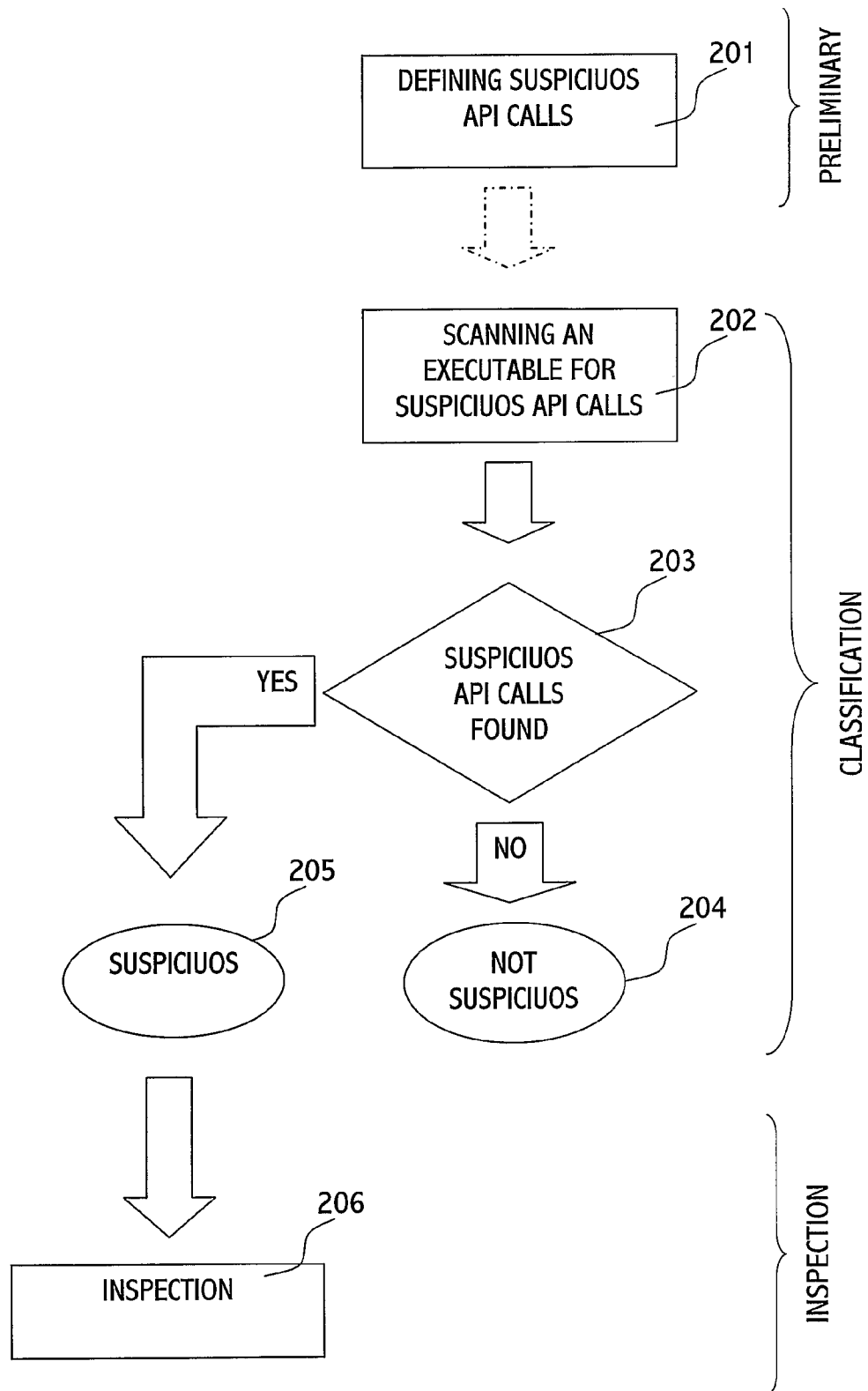


Fig. 1
PRIOR ART

**Fig. 2**

**Fig. 3**

Electronic Acknowledgement Receipt

EFS ID:	2679103
Application Number:	11428203
International Application Number:	
Confirmation Number:	3669
Title of Invention:	METHOD AND SYSTEM FOR CLASSIFICATION OF SOFTWARE USING CHARACTERISTICS AND COMBINATIONS OF SUCH CHARACTERISTICS
First Named Inventor/Applicant Name:	Ben Godwood
Customer Number:	23446
Filer:	Robert A. Mazzaresse/Timothy Grimes
Filer Authorized By:	Robert A. Mazzaresse
Attorney Docket Number:	17678US01
Receipt Date:	07-JAN-2008
Filing Date:	30-JUN-2006
Time Stamp:	15:26:31
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes) /Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Filed	SPHS-0007-P01_010508_Form1449.pdf	99475 1a2c6f00cd7a1cc879f7e6495af0c80bb6711dd2	no	1

Warnings:

Information:

This is not an USPTO supplied IDS fillable form					
2	Information Disclosure Statement Letter	SPHS-0007-P01_010508_ID SCommunication.pdf	75394 c1c6265e3c898cea7f3ad8a1179248ef71887800	no	2
Warnings:					
Information:					
3	Foreign Reference	FPReferenceA.pdf	798026 cd2c520f5a790c06987ab5d0acba9f11511211546	no	30
Warnings:					
Information:					
4	NPL Documents	NPLReferenceB.pdf	73259 1c54a1790664c73fe0dde24252ec20290a0e9dccc	no	3
Warnings:					
Information:					
Total Files Size (in bytes):			1046154		
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(c) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
11/428,203	06/30/2006	Ben Godwood	17678US01

CONFIRMATION NO. 3669

23446
MCANDREWS HELD & MALLOY, LTD
500 WEST MADISON STREET
SUITE 3400
CHICAGO, IL 60661

Title: METHOD AND SYSTEM FOR CLASSIFICATION OF SOFTWARE USING CHARACTERISTICS AND COMBINATIONS OF SUCH CHARACTERISTICS

Publication No. US-2008-0005796-A1

Publication Date: 01/03/2008

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publicly available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently <http://www.uspto.gov/patft/>.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently <http://pair.uspto.gov/>. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
 United States Patent and Trademark Office
 Address: COMMISSIONER FOR PATENTS
 P.O. Box 1450
 Alexandria, Virginia 22313-1450
 www.uspto.gov

APPLICATION NUMBER	FILING OR 371 (c) DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET NUMBER
11/428,203	06/30/2006	Ben Godwood	17678US01

CONFIRMATION NO. 3669

FORMALITIES
 LETTER

23446
 MCANDREWS HELD & MALLOY, LTD
 500 WEST MADISON STREET
 SUITE 3400
 CHICAGO, IL 60661

Date Mailed: 07/26/2006

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

*Filing Date Granted***Items Required To Avoid Abandonment:**

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items and pay any fees required below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The oath or declaration is missing. *A properly signed oath or declaration in compliance with 37 CFR 1.63, identifying the application by the above Application Number and Filing Date, is required.*
Note: If a petition under 37 CFR 1.47 is being filed, an oath or declaration in compliance with 37 CFR 1.63 signed by all available joint inventors, or if no inventor is available by a party with sufficient proprietary interest, is required.

The applicant needs to satisfy supplemental fees problems indicated below.

The required item(s) identified below must be timely submitted to avoid abandonment:

- To avoid abandonment, a surcharge (for late submission of filing fee, search fee, examination fee or oath or declaration) as set forth in 37 CFR 1.16(f) of \$130 for a non-small entity, must be submitted with the missing items identified in this letter.

SUMMARY OF FEES DUE:

Total additional fee(s) required for this application is **\$130** for a Large Entity

- **\$130** Surcharge.

Replies should be mailed to: Mail Stop Missing Parts

Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

*A copy of this notice **MUST** be returned with the reply.*



Office of Initial Patent Examination (571) 272-4000, or 1-800-PTO-9199, or 1-800-972-6382
PART 2 - COPY TO BE RETURNED WITH RESPONSE

**COMBINED DECLARATION AND POWER OF ATTORNEY
FOR PATENT APPLICATION**

As a below-named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if several names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

**Method and System for Classification of Software Using Characteristics and Combinations
of Such Characteristics**

filed on June 30, 2006 as Application Serial No. 11.428,203.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with 37 CFR §1.56.

I hereby claim foreign priority benefits under 35 U.S.C. §119 (a)-(d) or (f) or 365(b) of any foreign application(s) for patent or inventor's or plant breeder's rights certificate(s), or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below, and have also identified below, by checking the box, any foreign application for patent, inventor's or plant breeder's rights certificate(s), or any PCT international application having a filing date before that of the application on which priority is claimed:

COUNTRY	APPLICATION NUMBER	DATE OF FILING (day, month, year)	PRIORITY NOT CLAIMED	CERTIFIED COPY ATTACHED
				<input type="checkbox"/> Yes <input type="checkbox"/> No
				<input type="checkbox"/> Yes <input type="checkbox"/> No
				<input type="checkbox"/> Yes <input type="checkbox"/> No

I hereby claim the benefit under 35 U.S.C. §120 of any United States application(s), or 365(c) of any PCT International application designating the United States of America, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of 35 U.S.C. §112, I acknowledge the duty to disclose material information as defined in 37 CFR §1.56 which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

U.S. PARENT APPLICATION OR PCT PARENT NUMBER	PARENT FILING DATE (day, month, year)	STATUS (patent and number, pending, abandoned)

I hereby claim the benefit under 35 U.S.C. §119(e) of any United States provisional application(s) listed below.

APPLICATION NUMBER(S)	FILING DATE (day, month, year)

As a named inventor, I hereby appoint Practitioners at Customer Number 23446 jointly, and each of them severally, my/our attorney(s) or agents(s), with full power of substitution, delegation and revocation, to prosecute this application, to make alterations and amendments therein, to receive the patent and to transact all business in the Patent and Trademark Office connected therewith.

I hereby direct that all correspondence and telephone calls in connection with this application be addressed to Practitioners at Customer Number 23446.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further, statements were made with the knowledge that willfully false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. §1001 and that all such willful false statements may jeopardize the validity of the application or any patent issued thereon.

This declaration names 2 inventors below.

Docket No. 17678US01

Full name of first joint inventor: Ben Godwood

Inventor's signature: Ben Godwood Date: 9/8/2006

Residence: 9 Hill Crescent
Finstock OX7 3BT, United Kingdom

Citizenship: British

Post Office Address: Same

Full name of second joint inventor: William James McCourt

Inventor's signature: W J McCourt Date: 9/8/06

Residence: 31 Galley Field
Abingdon OX14 3RU, United Kingdom

Citizenship: British

Post Office Address: Same

Electronic Patent Application Fee Transmittal

Application Number:	11428203			
Filing Date:	30-Jun-2006			
Title of Invention:	METHOD AND SYSTEM FOR CLASSIFICATION OF SOFTWARE USING CHARACTERISTICS AND COMBINATIONS OF SUCH CHARACTERISTICS			
First Named Inventor:	Ben Godwood			
Filer:	Christopher Neith George/Margaret Slavik			
Attorney Docket Number:	17678US01			
Filed as Large Entity				
Utility Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Processing Fee, except for Provis. apps	1808	1	130	130
Total in USD (\$)				130

Electronic Acknowledgement Receipt

EFS ID:	1149085
Application Number:	11428203
Confirmation Number:	3669
Title of Invention:	METHOD AND SYSTEM FOR CLASSIFICATION OF SOFTWARE USING CHARACTERISTICS AND COMBINATIONS OF SUCH CHARACTERISTICS
First Named Inventor:	Ben Godwood
Customer Number:	23446
Filer:	Christopher Neith George/Margaret Slavik
Filer Authorized By:	Christopher Neith George
Attorney Docket Number:	17678US01
Receipt Date:	10-AUG-2006
Filing Date:	30-JUN-2006
Time Stamp:	13:22:58
Application Type:	Utility
International Application Number:	

Payment information:

Submitted with Payment	yes
Payment was successfully received in RAM	\$ 130
RAM confirmation Number	834
Deposit Account	130017
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 and 1.17	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)	Multi Part	Pages
1	Applicant Response to Pre-Exam Formalities Notice	NoticeOfMissingParts.pdf	74243	no	2
Warnings:					
Information:					
2	Oath or Declaration filed	Declaration.pdf	123927	no	4
Warnings:					
Information:					
3	Fee Worksheet (PTO-875)	fee-info.pdf	8240	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			206410		
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p>					



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
 United States Patent and Trademark Office
 Address: COMMISSIONER FOR PATENTS
 P.O. Box 1450
 Alexandria, Virginia 22313-1450
 www.uspto.gov

APPLICATION NUMBER	FILING OR 371 (c) DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET NUMBER
11/428,203	06/30/2006	Ben Godwood	17678US01

23446
 MCANDREWS HELD & MALLOY, LTD
 500 WEST MADISON STREET
 SUITE 3400
 CHICAGO, IL 60661

CONFIRMATION NO. 3669

FORMALITIES
 LETTER

Date Mailed: 07/26/2006

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

*Filing Date Granted***Items Required To Avoid Abandonment:**

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items and pay any fees required below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The oath or declaration is missing. *A properly signed oath or declaration in compliance with 37 CFR 1.63, identifying the application by the above Application Number and Filing Date, is required.*
Note: If a petition under 37 CFR 1.47 is being filed, an oath or declaration in compliance with 37 CFR 1.63 signed by all available joint inventors, or if no inventor is available by a party with sufficient proprietary interest, is required.

The applicant needs to satisfy supplemental fees problems indicated below.

The required item(s) identified below must be timely submitted to avoid abandonment:

- To avoid abandonment, a surcharge (for late submission of filing fee, search fee, examination fee or oath or declaration) as set forth in 37 CFR 1.16(f) of \$130 for a non-small entity, must be submitted with the missing items identified in this letter.

SUMMARY OF FEES DUE:

Total additional fee(s) required for this application is **\$130** for a Large Entity

- **\$130** Surcharge.

Replies should be mailed to: Mail Stop Missing Parts

08/24/2006 VVAN11 00000008 130017 11428203

01 FC:1051 130.00 DA

Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

*A copy of this notice **MUST** be returned with the reply.*



Office of Initial Patent Examination (571) 272-4000, or 1-800-PTO-9199, or 1-800-972-6382
PART 2 - COPY TO BE RETURNED WITH RESPONSE



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
 United States Patent and Trademark Office
 Address: COMMISSIONER FOR PATENTS
 P.O. Box 1450
 Alexandria, Virginia 22313-1450
 www.uspto.gov

APPLICATION NUMBER	FILING OR 371 (c) DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET NUMBER
11/428,203	06/30/2006	Ben Godwood	17678US01

CONFIRMATION NO. 3669

FORMALITIES
 LETTER

23446
 MCANDREWS HELD & MALLOY, LTD
 500 WEST MADISON STREET
 SUITE 3400
 CHICAGO, IL 60661

Date Mailed: 07/26/2006

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

*Filing Date Granted***Items Required To Avoid Abandonment:**

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items and pay any fees required below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The oath or declaration is missing. *A properly signed oath or declaration in compliance with 37 CFR 1.63, identifying the application by the above Application Number and Filing Date, is required.*
Note: If a petition under 37 CFR 1.47 is being filed, an oath or declaration in compliance with 37 CFR 1.63 signed by all available joint inventors, or if no inventor is available by a party with sufficient proprietary interest, is required.

The applicant needs to satisfy supplemental fees problems indicated below.

The required item(s) identified below must be timely submitted to avoid abandonment:

- To avoid abandonment, a surcharge (for late submission of filing fee, search fee, examination fee or oath or declaration) as set forth in 37 CFR 1.16(f) of \$130 for a non-small entity, must be submitted with the missing items identified in this letter.

SUMMARY OF FEES DUE:

Total additional fee(s) required for this application is **\$130** for a Large Entity

- **\$130** Surcharge.

Replies should be mailed to: Mail Stop Missing Parts

Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

A copy of this notice MUST be returned with the reply.



Office of Initial Patent Examination (571) 272-4000, or 1-800-PTO-9199, or 1-800-972-6382
PART 3 - OFFICE COPY

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	17678US01
		Application Number	
Title of Invention	METHOD AND SYSTEM FOR CLASSIFICATION OF SOFTWARE USING CHARACTERISTICS AND COMBINATIONS OF SUCH CHARACTERISTICS		
<p>The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.</p> <p>This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.</p>			

Secrecy Order 37 CFR 5.2

- ☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Applicant Information:

Applicant 1					Remove
Applicant Authority		<input checked="" type="radio"/> Inventor		<input type="radio"/> Legal Representative under 35 U.S.C. 117	
				<input type="radio"/> Party of Interest under 35 U.S.C. 118	
Prefix	Given Name	Middle Name	Family Name	Suffix	
	Ben		Godwood		
Residence Information (Select One) <input type="radio"/> US Residency <input checked="" type="radio"/> Non US Residency <input type="radio"/> Active US Military Service					
City	Finstock	Country Of Residenceⁱ	GB		
Citizenship under 37 CFR 1.41(b)ⁱ		GB			
Mailing Address of Applicant:					
Address 1	9 Hill Crescent				
Address 2					
City	Finstock	State/Province			
Postal Code	OX7 3BT	Countryⁱ	GB		
Applicant 2					Remove
Applicant Authority		<input checked="" type="radio"/> Inventor		<input type="radio"/> Legal Representative under 35 U.S.C. 117	
				<input type="radio"/> Party of Interest under 35 U.S.C. 118	
Prefix	Given Name	Middle Name	Family Name	Suffix	
	William	James	McCourt		
Residence Information (Select One) <input type="radio"/> US Residency <input checked="" type="radio"/> Non US Residency <input type="radio"/> Active US Military Service					
City		Country Of Residenceⁱ	GB		
Citizenship under 37 CFR 1.41(b)ⁱ		GB			
Mailing Address of Applicant:					
Address 1	31 Galley Field				
Address 2					
City	Abingdon	State/Province			
Postal Code	OX14 3RU	Countryⁱ	GB		
All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the Add button.					Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

- ☐ An Address is being provided for the correspondence Information of this application.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	17678US01
		Application Number	
Title of Invention	METHOD AND SYSTEM FOR CLASSIFICATION OF SOFTWARE USING CHARACTERISTICS AND COMBINATIONS OF SUCH CHARACTERISTICS		
Customer Number	23446		
Email Address		<input type="button" value="Add Email"/>	<input type="button" value="Remove Email"/>

Application Information:

Title of the Invention	METHOD AND SYSTEM FOR CLASSIFICATION OF SOFTWARE USING CHARACTERISTICS AND COMBINATIONS OF SUCH CHARACTERISTICS		
Attorney Docket Number	17678US01	Small Entity Status Claimed	<input type="checkbox"/>
Application Type	Nonprovisional		
Subject Matter	Utility		
Suggested Class (if any)		Sub Class (if any)	
Suggested Technology Center (if any)			
Total Number of Drawing Sheets (if any)		Suggested Figure for Publication (if any)	
Publication Information:			
<input type="checkbox"/> Request Early Publication (Fee required at time of Request 37 CFR 1.219)			
<input type="checkbox"/> Request Not to Publish. I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application has not been and will not be the subject of an application filed in another country, or under a multilateral agreement, that requires publication at eighteen months after filing.			

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32). Enter either Customer Number or complete the Representative Name section below. If both sections are completed the Customer Number will be used for the Representative Information during processing.			
Please Select One:	<input checked="" type="radio"/> Customer Number	<input type="radio"/> US Patent Practitioner	<input type="radio"/> US Representative (37 CFR 11.9)
Customer Number	23446		

Domestic Priority Information:

This section allows for the applicant to claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c). Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78(a)(2) or CFR 1.78(a)(4), and need not otherwise be made part of the specification.			
Prior Application Status		<input type="button" value="Remove"/>	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
Additional Domestic Priority Data may be generated within this form by selecting the Add button.			<input type="button" value="Add"/>

Foreign Priority Information:

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	17678US01
		Application Number	
Title of Invention	METHOD AND SYSTEM FOR CLASSIFICATION OF SOFTWARE USING CHARACTERISTICS AND COMBINATIONS OF SUCH CHARACTERISTICS		

This section allows for the applicant to claim benefit of foreign priority and to identify any prior foreign application for which priority is not claimed. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(a).

			Remove
Application Number	Country ⁱ	Parent Filing Date (YYYY-MM-DD)	Priority Claimed
			<input type="radio"/> Yes <input checked="" type="radio"/> No
Additional Foreign Priority Data may be generated within this form by selecting the Add button.			Add

Assignee Information:

Providing this information in the application data sheet does not substitute for compliance with any requirement of part 3 of Title 37 of the CFR to have an assignment recorded in the Office.

Assignee 1					Remove
If the Assignee is an Organization check here. <input type="checkbox"/>					
Prefix	Given Name	Middle Name	Family Name	Suffix	
Mailing Address Information:					
Address 1					
Address 2					
City		State/Province			
Country ⁱ		Postal Code			
Phone Number		Fax Number			
Email Address					
Additional Assignee Data may be generated within this form by selecting the Add button.					Add

Signature:

A signature of the applicant or representative is required in accordance with 37 CFR 1.33 and 10.18. Please see 37 CFR 1.4(d) for the form of the signature.

Signature	/Christopher N. George/		Date (YYYY-MM-DD)	2006-06-30
First Name	Christopher	Last Name	George	Registration Number
				51728

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Attorney Docket Number 17678US01

Date of Deposit: June 30, 2006

Attorney Docket No.17678US01

5 METHOD AND SYSTEM FOR CLASSIFICATION OF SOFTWARE USING
CHARACTERISTICS AND COMBINATIONS OF SUCH CHARACTERISTICS

RELATED APPLICATIONS

[01] [Not Applicable]

FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT

10 [02] [Not Applicable]

MICROFICHE/COPYRIGHT REFERENCE

[03] [Not Applicable]

BACKGROUND OF THE INVENTION

[04] The present invention generally relates to classification of software, including malware and unwanted software. More particularly, the present invention relates to identification of software based on identification of certain characteristics (hereinafter
5 called “genes”) and matching such genes against certain created classifications defined as groupings of genes.

[05] Malware is a general categorization of a computer contaminant including computer viruses, worms, Trojan horses, spyware and/or adware, for example. Unlike defective software which has a legitimate purpose but contains errors, malware is written
10 to infiltrate or damage a computer system and/or other software. Malware may also steal sensitive information, such as passwords. Some malware programs install a key logger, which copies down the user's keystrokes when entering a password, credit card number, or other useful information.

[06] Malware includes viruses and worms, which spread to infect other executable
15 software and/or computers locally and/or over a network, for example. By inserting a copy of itself into the machine code instructions in these executables, a virus causes itself to be run whenever the program is run or the disk is booted.

[07] Additionally, Microsoft Word® and similar programs include flexible macro systems receptive to macro viruses that infect documents and templates, rather than
20 applications, through executable macro code.

[08] Worms, unlike viruses, typically do not insert themselves into other programs but, rather, exploit security holes in network server programs and start themselves running as

a separate process. Worms typically scan a network for computers with vulnerable network services, break in to those computers, and replicate themselves.

[09] Another type of malware is a Trojan horse or Trojan. Generally, a Trojan horse is an executable program that conceals a harmful or malicious payload. The payload may take effect immediately and can lead to many undesirable effects, such as deleting all the user's files, or the payload may install further harmful software into the user's system. Trojan horses known as droppers are used to start off a worm outbreak by injecting the worm into users' local networks.

[10] Spyware programs are produced for the purpose of gathering information about computer users.

[11] Additionally, systems may become infected with unwanted software. Unwanted software is defined as being software that is installed or used without the system owner's permission. Although unwanted software is not malicious, it can either affect performance of client machines or potentially introduce security risks and related legal risks into an organization. Such unwanted software may include adware, dialers, remote administration tools and hacking tools.

[12] Traditional malware protection techniques are based around anti-virus vendors creating signatures for known malware and products that scan systems searching for those specific signatures.

[13] With this approach, an identification or definition of malware and/or unwanted software is released once a lab has seen and analyzed a sample of such software. This can mean that some users may be infected before the definitions have been released. Thus,

systems and methods providing detection of unknown malware and/or unwanted software to help prevent users from being infected before a definition is released would be highly desirable.

[14] The volume of malware has increased dramatically (around 140+ Brazilian Banking Trojans per day for example). Multiple variants of the same malware threat are relentlessly created and rapidly distributed, with the aim of defeating traditional signature-based virus protection.

[15] Some anti-virus software uses heuristics to attempt to identify unknown viruses. Heuristics techniques look at various properties of a file and not necessarily the functionality of the program. This leads to high false positive rates.

[16] Other behavior based technologies rely on running malware and attempting to stop execution if malicious behavior is observed to happen. By allowing malware to execute, the malware may already have caused damage before it is blocked. Additionally, behavior-based technology often requires extensive user interaction to authorize false positives.

[17] The network security threats faced by enterprises today are much more complex than 20 years ago. The exponential growth in malware is compounded by its speed of propagation and the complexity of blended threats, changing the nature of the risks. The behavior of network users is also changing rapidly. There is a need for systems and methods for proactively classifying software before malware or unwanted software causes damage.

BRIEF SUMMARY OF THE INVENTION

[18] Certain embodiments of the present invention provide methods and systems for software classification.

[19] Certain embodiments provide a method for classifying software including identifying at least one of a functional block and a property of the software. The method further includes identifying one or more genes in the at least one of a functional block and a property of the software. Additionally, the method includes matching the one or more genes against one or more classifications defined from groupings of genes. Furthermore, the method includes classifying the software based on the one or more classifications.

[20] Certain embodiments provide a method for generating classifications defined for groupings of genes, for use in classifying software. The method includes identifying one or more genes that appear in software. The method further includes combining a plurality of genes to classify or form a set of genes. Additionally, the method includes testing the set of genes for false-positives against one or more reference files. The method also includes defining a software classification based on the set of genes.

[21] Certain embodiments provide a computer-readable medium having a set of instructions for execution on a computer. The set of instructions includes an identification routine configured to identify one or more functional blocks and/or properties of software. The set of instructions also includes a routine configured to identify genes in the one or more functional blocks and/or properties. Furthermore, the set of instructions includes a matching routine configured to match genes against a list of

Attorney Docket Number 17678US01

known classifications defined as groupings of genes. Additionally, the set of instructions includes a classification routine configured to classify the software.

BRIEF DESCRIPTION OF SEVERAL VIEWS OF THE DRAWINGS

[22] Figure 1 illustrates a malware detection system in accordance with an embodiment of the present invention.

[23] Figure 2 depicts a flow diagram for a method for software classification in accordance with an embodiment of the present invention.

[24] Figure 3 illustrates a flow diagram for a method for generating genes and groupings of genes for software classification in accordance with an embodiment of the present invention.

[25] The foregoing summary, as well as the following detailed description of certain embodiments of the present invention, will be better understood when read in conjunction with the appended drawings. For the purpose of illustrating the invention, certain embodiments are shown in the drawings. It should be understood, however, that the present invention is not limited to the arrangements and instrumentality shown in the attached drawings.

DETAILED DESCRIPTION OF THE INVENTION

[26] Figure 1 illustrates a malware detection system 100 in accordance with an embodiment of the present invention. System 100 includes a memory 110 storing one or more files, a malware detection engine 120, and a library 130. System 100 may also include an interface (not shown) to allow a user to interact with malware detection engine 120 to trigger a malware scan, view status, view results, take action, etc.

[27] Memory 110 may include a hard disk, a floppy disk, an optical disk, a magnetic disk, a tape, a random access memory (RAM), a read-only memory (ROM), a programmable ROM (PROM, EPROM, EEPROM), CD, DVD, flash memory, cache, buffer, register, and/or other temporary or persistent data storage. File(s) to be scanned may be temporarily and/or persistently stored in memory 110. Memory 110 may be normal computer system memory and/or special purpose memory for use in malware detection.

[28] Library 130 includes one or more of saved checksums, malware patterns, virus and/or other malware definitions, gene information, information as classifications based on groupings of genes, etc. Library 130 is accessed by malware engine 120 to detect/classify malware in a file.

[29] Components of system 100 may be implemented in software, hardware and/or firmware, for example. The components of system 100 may be implemented separately and/or implemented in a variety of combinations. For example, library 130 may be incorporate in malware engine 120. Components of system 100 may be implemented on a single computer system for processing software and messages. Alternatively,

components of system 100 may be implemented in a distributed network where different processes occur on different machines with a communication network to allow sharing of information. System 100 may be implemented using one or more software programs.

[30] In certain embodiments, system 100 provides both immediate and scheduled
5 malware scanning and disinfection. Malware may be detected in a variety of ways, such as by comparing checksum of a file to a stored checksum value, pattern matching to identify known malware patterns in files, electronic mail and/or disk areas (e.g., boot sectors), emulating all or part of a file's code to try and detect malware, such as polymorphic viruses, which may reveal themselves during execution, and/or extracting
10 and analyzing functionality from a file by matching genes and/or classifications defined from groupings of genes, e.g., PHENOTYPE™ classifications (PHENOTYPE™ is a trademark of the assignee of the present patent application). After detection, a user and/or system may be notified of detected malware, and system 100 may automatically and/or upon request attempt to disinfect, quarantine or remove detected malware or malware
15 fragments from the file/email/disk area.

[31] Pattern matching and other forms of detection may be performed using Virus Identity Files (IDEs) or other identity files that contain algorithms describing various characteristics of a virus and/or other malware for use in malware recognition.

[32] Malware engine 120 loads and searches data from the input file. Malware engine
20 120 may use pattern matching, for example, to compare sequences of code in the file to known virus code sequences identify a particular sequence of code that is similar or identical to a virus code. Malware engine 120 may also combine pattern matching with

heuristics to use general, rather than specific, rules to detect several viruses in the same family, for example. Malware engine 120 may also include a code emulator for detecting polymorphic viruses (self-modifying viruses) and/or an on-line decompressor for scanning inside archive files. Malware engine 120 may also include an OLE2 (object
5 linking and embedding) engine for detecting and disinfecting macro viruses.

[33] In certain embodiments, malware engine 120 receives an input file and returns a result. Virus IDE and product updates may be downloaded to account for new viruses and/or other malware, for example.

[34] In certain embodiments, malware engine 120 may be used to scan files “on-
10 demand.” A user may identify files or groups of files to scan immediately.

[35] On-demand scanning may also be scheduled by a user. For example, the user specifies a time at which to scan a selected group of files. At the scheduled time, malware engine 120 scans the selected files that are already stored, for example, in memory 110. A user or users may establish multiple schedules for malware scanning.
15 Different configurations may be set for each scheduled scan. Alternatively and/or in addition, certain embodiments provide on-access malware detection using malware engine 120.

[36] In certain embodiments, malware engine 120 intercepts open file or file close or file access requests, for example, by a user, an operating system, an application, etc.

[37] In certain embodiments, a user may specify which files to check via a scheduled
20 and/or on-access scan. That is, a user can include and/or exclude certain types of files from malware scanning. Additionally, the user may configure system 100 to check files

on read, on write, and/or on rename, for example. The user may also configure system 100 to block access to the file, or to automatically initiate disinfection, removal and/or quarantine of a file upon finding malware in the file.

[38] In certain embodiments, system 100 may be used to identify malware by extracting functionality from a file and classifying the functionality. In certain embodiments, malware engine 120 may classify functionality and identify malware without requiring a most up-to-date set of virus and/or other malware definitions. Malware engine 120 may classify a file and/or functionality within a file as malicious, non-malicious, suspicious, etc. based on functionality and/or relationships between or combinations of functionality, for example. Alternatively and/or in addition, malware engine 120 may identify a particular malware program represented by and/or included in the file.

[39] Figure 2 depicts a flow diagram for a method 200 for software classification in accordance with an embodiment of the present invention. At step 210, analysis of a computer file or other sample to be checked is commenced. At step 220, the file is filtered. This is a series of quick checks to determine whether a file needs further analysis. For example, one or more files may be screened for efficiency reasons. If a file is packed, for example, a malware detection system may spend more time checking the file. If a file passes a checksum test, for example, the software classification system may not further examine the file.

[40] In certain embodiments, at step 230, properties are extracted from the file. For example the file size or name may be extracted.

[41] In certain embodiments, the file is unpacked if necessary (step 240). For example, malware may be obfuscated using run-time packers, which render static analysis of code difficult. Packing is a process of transforming a program file, using compression and/or encryption, so that its functionality is obfuscated. Unpacking is a method of restoring a packed program file to its unpacked state, so that the functionality is no longer obfuscated. This is done using decompression and/or decryption, for example.

[42] At step 250, the function blocks are extracted from the file. These functional blocks include sequences of application program interface (API) calls, string references, etc., which illustrate the function and execution flow of the program. Functional blocks are extracted from a program file's binary code. While various instances of software may use common code and similar techniques, the resulting compiled bytes can be very different. The same source code can be compiled using different compilers to produce different binary files. The compiled bytes are different but the files are functionally the same. Functional blocks provide a high level view of the functionality of a file regardless of binary compilation.

[43] At step 260, each functional block is searched for genes to build a list of genes present in the file. Different types of functionality (classified as genes, for example) may be extracted from the sequenced blocks. A gene is piece of functionality or property of a program. Each piece of functionality is described using sequences of APIs and strings, which can be matched against functional blocks. A matching functional block includes the APIs and strings in the correct order. The gene and the functional block do not need to match exactly. A functional block may contain more than one gene. Genes are defined using a gene definition language, for example. Each gene describes or identifies a

different behavior or characteristic of malware or other file. For example, malware may copy itself to a %SYSTEM% directory. Therefore, a gene may be created to identify this functionality by matching the sequence of API calls and the strings that are referenced.

[44] At step 270, the list of genes is compared against a library of classifications of genes. A classification of gene combination has been detected if all the genes contained in that gene combination are present in the list of genes identified in the file.

[45] A classification of genes represents a certain class of software. A classification of genes is a combination of genes used to describe or identify a class of software program. For example, a classification of genes to match an IRC Bot malware file (an independent program that connects to an Internet Relay Chat (IRC) and performs automated functions) may include the following genes:

SocketSend	- Socket based activity
RunKey	- Sets a run key
Exec	- Executes other programs
CopySys	- Copies itself to the system directory
AVList	- Contains a list of AV (anti-virus) products
IRC	- IRC references
Host	- References the hosts file

[46] At step 280, an output is generated. For example, the most significant classification may be reported. Alternatively and/or in addition, all identified classifications, genes and/or software classifications may be reported. Reporting may include generating and/or editing a log file, printing an output, emailing an output, generating an audible output, generating a visual output, facsimile transmission of an output, electronic storage of an output, etc. In addition to reporting, an output may

include disinfection, deletion, and/or quarantine of the file and/or related files, for example.

[47] For example, the following functional block sequenced from a software program matches three genes (“CopySys”, “Runkey” and “Exec”):

5 GetSystemDirectoryA
 GetModuleHandleA
 GetModuleFileNameA
 "tftpd.exe"
 "winhlpp32.exe"
10 strcat
 strcat
 "software\microsoft\windows\currentversion\run"
 RegCreateKeyExA
 strlen
15 RegSetValueExA
 RegCloseKey
 CopyFileA
 CreateProcessA

20 The gene “CopySys” copies itself to a system folder and includes the following functions,
 for example:

 GetSystemDirectoryA
 GetModuleHandleA
25 GetModuleFileNameA
 ".exe"
 CopyFileA

 The gene “Runkey” sets a run key and includes, as an example, the following functions:
30 "software\microsoft\windows\currentversion\run"
 RegCreateKeyExA
 RegSetValueExA

35 The gene “Exec” executes other programs and includes, as an example, the following
 functions:

 CreateProcessA

The three genes in this example form a classification defined by a group of the three genes, and may be used to classify the software as malicious, suspicious, unwanted, etc.

[48] Figure 3 illustrates a flow diagram for a method 300 for generating genes and classifications defined by groupings of genes to be used for malware and/or other software classification in accordance with an embodiment of the present invention. At step 310, software functionality is identified. For example, the functionality for copying code to a system directory is identified. At step 320, a software characteristic is defined based on the identified functionality. For example, the characteristic 'CopySys' from the above example is defined based on the identified copy functionality.

[49] At step 330, a plurality of software characteristics are combined to form a software classification. For example, the characteristics listed in the examples above: 'SockSend, RunKey, Exec, CopySys, AVList, IRC, and Host' are combined to form a classification for an 'IRC Bot' program.

[50] In certain embodiments, functionality is common to both malware and normal programs. Malware may be identified and/or classified based on combinations of such functionality. In certain embodiments, both malware and non-malware programs may be classified according to a variety of genes and/or groupings of genes. For example, unwanted software may be classified according to extracted functionality.

[51] Thus, certain embodiments provide systems and methods to extract functionality of a file to identify malware and/or other types of software programs. Certain embodiments may be used to find functionally similar files, such as by using a "Query by Functionality" search. Certain embodiments detect malware without requiring new

patterns to be written for pattern matching detection. Certain embodiments reduce a false positive rate by matching on functionality, rather than heuristics, to describe a type of malware. Certain embodiments allow computers and/or software to be checked for licensing compliance and software updates.

5 **[52]** While the invention has been described with reference to certain embodiments, it will be understood by those skilled in the art that various changes may be made and equivalents may be substituted without departing from the scope of the invention. In addition, many modifications may be made to adapt a particular situation or material to the teachings of the invention without departing from its scope. Therefore, it is intended
10 that the invention not be limited to the particular embodiment disclosed, but that the invention will include all embodiments falling within the scope of the appended claims.

CLAIMS

1. A method for classifying software, said method comprising:

identifying at least one of a functional block and a property of said software;

5 identifying one or more genes in said at least one of a functional block and a property of said software;

matching said one or more genes against one or more classifications defined by a groupings of genes; and

classifying said software based on said one or more classifications.

10

2. The method of claim 1, wherein said classifying step further comprises classifying said software as malware based on said one or more classifications.

3. The method of claim 1, wherein said classifying step further comprises

15 classifying said software as unwanted software.

4. The method of claim 1, further comprising unpacking said software.

5. The method of claim 1, further comprising disassembling said software.

20

6. The method of claim 1, further comprising filtering said software.

7. The method of claim 1, further comprising unencrypting said software.

8. The method of claim 1, further comprising generating an output based on said classifying of said software.

5 9. The method of claim 1, further comprising disinfecting at least one of said software and a computer when said software is classified as malware.

10. The method of claim 1, further comprising removing said software when said software is classified as malware or unwanted software.

10

11. The method of claim 1, further comprising quarantining said software when said software is classified as malware or unwanted software.

12. The method of claim 1, further comprising generating reports regarding said software.

15

13. The method of claims 1, further comprising blocking access to said software when said software is classified as malware or unwanted software.

20 14. The method of claim 1, further comprising scanning a computer for said software, wherein said scanning include user initiated scanning, scheduled scanning and on-access scanning.

15. The method of claim 1, wherein said classification is based upon one or more groupings of genes.

16. A method for generating software classifications for use in classifying software, said method comprising:

identifying one or more genes that appear in software;

combining a plurality of genes to form a set of genes;

testing said set of genes for false-positives against one or more reference files; and

defining a software classification based on said set of genes.

17. The method of claim 16, wherein said software classification classifies malware.

18. The method of claim 16, wherein said software classification classifies unwanted software.

19. A computer-readable medium having a set of instructions for execution on a computer, said set of instructions comprising:

an identification routine configured to identify one or more functional blocks and/or properties of software;

a routine configured to identify genes in said one or more functional blocks and/or properties;

a matching routine configured to match genes against a list of predetermined classifications defined by groupings of genes; and

a classification routine configured to classify said software.

5 20. The set of instructions of claim 19, wherein said classification routine is configured to classify malware.

21. The set of instructions of claim 19, wherein said classification routine is configured to classify unwanted software.

10

22. The set of instructions of claim 19, further comprising an unpacking routine configured to unpack said software.

23. The set of instructions of claim 19, further comprising a disassembly
15 routine configured to disassemble said software.

24. The set of instructions of claim 19, further comprising a filtering routine configured to filter said software.

20 25. The set of instructions of claim 19, further comprising an unencryption routine configured to unencrypt said software.

26. The set of instructions of claim 19, further comprising an output routine configured to generate an output based on a classification of said software.

27. The set of instructions of claim 19, further comprising a disinfection routine configured to disinfect said software when said software is classified as malware.

28. The set of instructions of claim 19, further comprising a removal routine configured to remove said software when said software is classified as malware or unwanted software.

29. The set of instructions of claim 19, further comprising a quarantine routine configured to quarantine said software when said software is classified as malware or unwanted software.

30. The set of instructions of claim 19, further comprising a reporting routine configured to generate reports regarding said software.

31. The set of instructions of claim 19, further comprising a blocking routine configured to block access to said software when said software is classified as malware or unwanted software.

32. The set of instructions of claim 19, further comprising a scanning routine configured to scan a computer for said software, said scanning including at least one of

user initiated scanning, scheduled scanning and on-access scanning.

33. The set of instructions of claim 19, further comprising a classification generation routine configured to generate software classifications, said classification routine executing the steps of:

identifying a software functionality;

defining a characteristic based on said identified software functionality; and

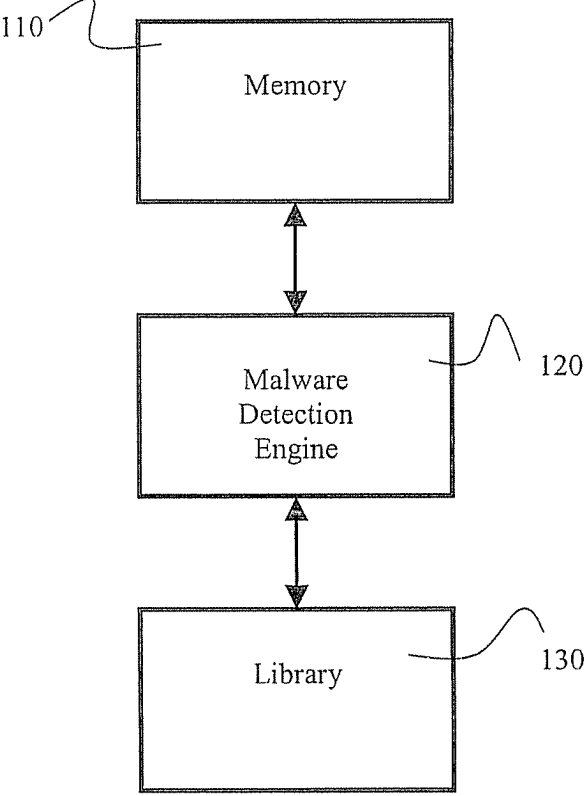
combining a plurality of characteristics to form a classification.

ABSTRACT OF THE DISCLOSURE

[53] Certain embodiments of the present invention provide methods and systems for software classification. Certain embodiments provide a method for identification of malware. Certain embodiments provide a method for identification of unwanted software. The method includes identifying one or more functional blocks and/or properties of software. The method further includes identifying genes in the functional blocks and/or properties. The method also includes matching the resulting list of genes against one or more combinations of classifications of groupings of genes. Additionally, the method includes classifying the software. Certain embodiments provide a method for generating classifications. The method includes identifying functional blocks and/or properties. Furthermore, the method includes combining a plurality of genes to form a classification.

Figure 1

100



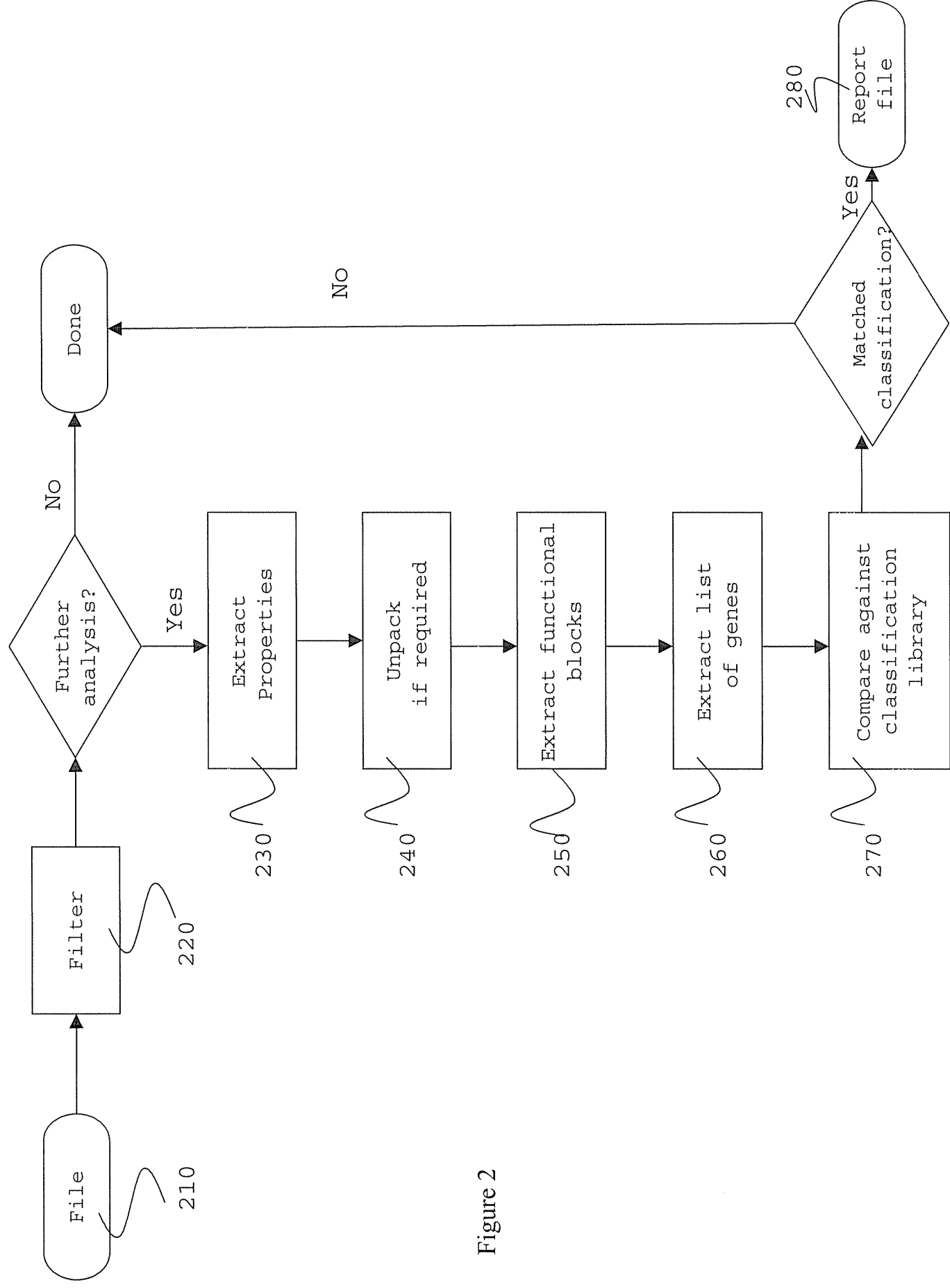
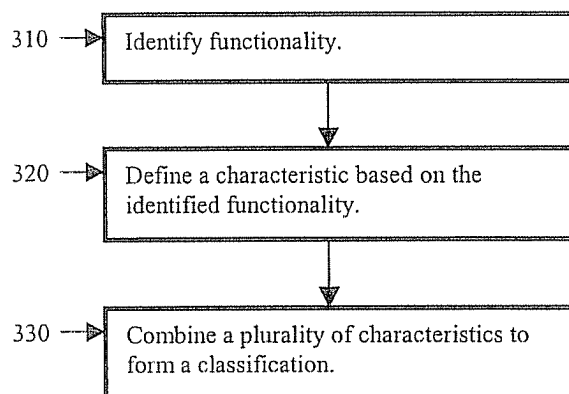


Figure 2

Figure 3
300



Electronic Patent Application Fee Transmittal

Application Number:				
Filing Date:				
Title of Invention:	METHOD AND SYSTEM FOR CLASSIFICATION OF SOFTWARE USING CHARACTERISTICS AND COMBINATIONS OF SUCH CHARACTERISTICS			
First Named Inventor:	Ben Godwood			
Filer:	Christopher Neith George/Margaret Slavik			
Attorney Docket Number:	17678US01			
Filed as Large Entity				
Utility Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Utility application filing	1011	1	300	300
Utility Search Fee	1111	1	500	500
Utility Examination Fee	1311	1	200	200
Pages:				
Claims:				
Claims in excess of 20	1202	13	50	650
Miscellaneous-Filing:				
Petition:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				1650

Electronic Acknowledgement Receipt

EFS ID:	1100451
Application Number:	11428203
Confirmation Number:	3669
Title of Invention:	METHOD AND SYSTEM FOR CLASSIFICATION OF SOFTWARE USING CHARACTERISTICS AND COMBINATIONS OF SUCH CHARACTERISTICS
First Named Inventor:	Ben Godwood
Customer Number:	23446
Filer:	Christopher Neith George/Margaret Slavik
Filer Authorized By:	Christopher Neith George
Attorney Docket Number:	17678US01
Receipt Date:	30-JUN-2006
Filing Date:	
Time Stamp:	18:09:37
Application Type:	Utility
International Application Number:	

Payment information:

Submitted with Payment	yes
Payment was successfully received in RAM	\$ 1650
RAM confirmation Number	533
Deposit Account	130017
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 and 1.17	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)	Multi Part	Pages
1	Application Data Sheet	ApplicationDataSheet.pdf	1437211	no	4
Warnings:					
Information:					
2		Specification.pdf	898633	yes	23
	Multipart Description				
	Doc Desc		Start	End	
	Specification		1	16	
	Claims		17	22	
	Abstract		23	23	
Warnings:					
Information:					
3	Drawings	Drawings.pdf	45773	no	3
Warnings:					
Information:					
4	Fee Worksheet (PTO-875)	fee-info.pdf	8527	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			2390144		
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p>					

Electronic Acknowledgement Receipt

EFS ID:	1100451
Application Number:	11428203
Confirmation Number:	3669
Title of Invention:	METHOD AND SYSTEM FOR CLASSIFICATION OF SOFTWARE USING CHARACTERISTICS AND COMBINATIONS OF SUCH CHARACTERISTICS
First Named Inventor:	Ben Godwood
Customer Number:	23446
Filer:	Christopher Neith George/Margaret Slavik
Filer Authorized By:	Christopher Neith George
Attorney Docket Number:	17678US01
Receipt Date:	30-JUN-2006
Filing Date:	
Time Stamp:	18:09:37
Application Type:	Utility
International Application Number:	

Payment information:

Submitted with Payment	yes
Payment was successfully received in RAM	\$ 1650
RAM confirmation Number	533
Deposit Account	130017
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 and 1.17	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)	Multi Part	Pages
1	Application Data Sheet	ApplicationDataSheet.pdf	1437211	no	4
Warnings:					
Information:					
2		Specification.pdf	898633	yes	23
	Multipart Description				
	Doc Desc		Start	End	
	Specification		1	16	
	Claims		17	22	
	Abstract		23	23	
Warnings:					
Information:					
3	Drawings	Drawings.pdf	45773	no	3
Warnings:					
Information:					
4	Fee Worksheet (PTO-875)	fee-info.pdf	8527	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			2390144		
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p>					

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD					Application or Docket Number 11428203	
Substitute for Form PTO-875						
APPLICATION AS FILED – PART I						
(Column 1)		(Column 2)		SMALL ENTITY		OR
OTHER THAN SMALL ENTITY						
FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)	RATE (\$)	FEE (\$)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A		N/A	300
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A		N/A	500
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A		N/A	200
TOTAL CLAIMS (37 CFR 1.16(i))	33	minus 20 = * 13	X 25=		X 50=	650
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3	minus 3 = *	X 100=		X 200=	
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR					
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))			N/A		N/A	
			TOTAL		TOTAL	1650
* If the difference in column 1 is less than zero, enter "0" in column 2.						
APPLICATION AS AMENDED – PART II						
(Column 1)		(Column 2)		(Column 3)		
AMENDMENT A	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	SMALL ENTITY		OR
	Total (37 CFR 1.16(i))	Minus **	=	RATE (\$)	ADDITIONAL FEE (\$)	OTHER THAN SMALL ENTITY
	Independent (37 CFR 1.16(h))	Minus ***	=	RATE (\$)	ADDITIONAL FEE (\$)	
	Application Size Fee (37 CFR 1.16(s))			X =		X =
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))			X =		X =
			N/A		N/A	
			TOTAL		TOTAL	
			ADD'T FEE		ADD'T FEE	
(Column 1)		(Column 2)		(Column 3)		
AMENDMENT B	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	SMALL ENTITY		OR
	Total (37 CFR 1.16(i))	Minus **	=	RATE (\$)	ADDITIONAL FEE (\$)	OTHER THAN SMALL ENTITY
	Independent (37 CFR 1.16(h))	Minus ***	=	RATE (\$)	ADDITIONAL FEE (\$)	
	Application Size Fee (37 CFR 1.16(s))			X =		X =
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))			X =		X =
			N/A		N/A	
			TOTAL		TOTAL	
			ADD'T FEE		ADD'T FEE	
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3. ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3". The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.						

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.