



- (51) International Patent Classification:
G06F 21/56 (2013.01)
- (21) International Application Number:
PCT/CN2013/090623
- (22) International Filing Date:
27 December 2013 (27.12.2013)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
201310239124.0 17 June 2013 (17.06.2013) CN
- (71) Applicant: **TENCENT TECHNOLOGY (SHENZHEN) COMPANY LIMITED** [CN/CN]; Room 403, East Block 2, SEG Park, Zhenxing Road, Futian District, Shenzhen, Guangdong 518000 (CN).
- (72) Inventor: **SHI, Youdi**; Room 403, East Block 2, SEG Park, Zhenxing Road, Futian District, Shenzhen, Guangdong 518000 (CN).
- (74) Agent: **SHENPAT INTELLECTUAL PROPERTY AGENCY**; Room 1521, West Block, Guomao Building, Shenzhen, Guangdong 518014 (CN).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— with international search report (Art. 21(3))

(54) Title: METHOD AND DEVICE FOR SEARCHING FOR PARENT VIRUS

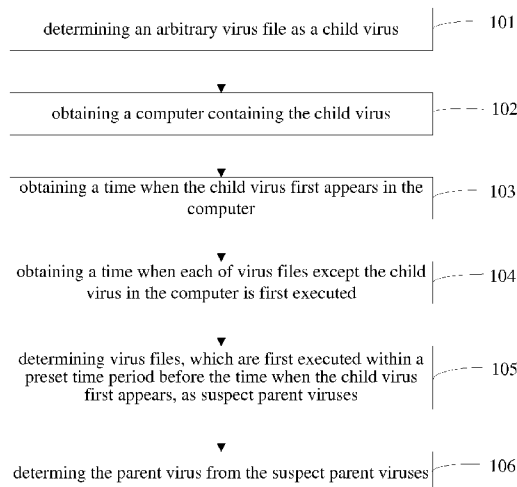


Fig. 1

(57) Abstract: A method and a device for searching for a parent virus are disclosed. The method includes: determining an arbitrary virus file as a child virus; obtaining a computer containing the child virus; obtaining a time when the child virus first appears in the computer; obtaining a time when each of virus files except the child virus in the computer is first executed; determining virus files, which are first executed within a preset time period before the time when the child virus first appears, as suspect parent viruses; and determining, from the suspect parent viruses, the parent viruses. Based on a principle that the time when the parent virus is executed is earlier than the time when the child virus first appears, the suspect parent viruses are determined, and the parent virus is found from the suspect parent viruses accurately.



METHOD AND DEVICE FOR SEARCHING FOR PARENT VIRUS

[0001] The present application claims the priority to Chinese Patent Application No. 201310239124.0, entitled as “METHOD AND DEVICE FOR SEARCHING FOR PARENT
5 VIRUS”, filed on June 17, 2013 with State Intellectual Property Office of People’s Republic of China, which is incorporated herein by reference in its entirety.

TECHNICAL FIELD

[0002] The present disclosure relates to network security, and in particular, to a method and a device for searching for a parent virus.

10 BACKGROUND

[0003] Technologies of computer viruses are developing with the development of computer technologies, and accordingly network security is threatened. There are various computer viruses, and most of them exist in the form of file. Some virus files may generate other computer virus files by, for example, loading files or creating files. The virus file generating
15 other computer virus file is referred to as a parent virus, and the generated computer virus file is referred to as a child virus. In view of the above, the parent virus is capable of spreading viruses, and the viruses may be completely removed only if the parent virus of the child viruses is found and removed.

[0004] Currently, the parent virus is searched for by monitoring approaches with which the
20 parent virus generates the child viruses. However, some parent viruses generate child viruses with complicated approaches including such as loading files, creating files, driving and tampering Master Boot Record (MBR), and the monitoring may be evaded. Therefore, it is difficult to find the parent virus by monitoring the approaches with which the parent virus generates the child viruses.

25 SUMMARY

[0005] A method and a device for searching for a parent virus are provided by the

disclosure, for accurately searching for the parent virus.

[0006] A method for searching for a parent virus is provided. The method includes:

determining an arbitrary virus file as a child virus;

obtaining a computer containing the child virus;

5 obtaining a time when the child virus first appears in the computer;

obtaining a time when each of virus files except the child virus in the computer is first executed;

determining virus files, which are first executed within a preset time period before the time when the child virus first appears, as suspect parent viruses; and

10 determining, from the suspect parent viruses, the parent virus.

[0007] Optionally, the method may further include, after the determining virus files, which are first executed within a preset time period before the time when the child virus first appears, as suspect parent viruses, and before the determining, from the suspect parent viruses, the parent virus,

15 obtaining extent of each of the suspect parent viruses;

sequencing the suspect parent viruses in descending order based on the extent of each of the suspect parent viruses; and

obtaining the first n suspect parent viruses, where n is a preset natural number, and

the determining, from the suspect parent viruses, the parent virus includes:

20 determining, from the first n suspect parent viruses, the parent virus.

[0008] Optionally, the determining, from the suspect parent viruses, the parent virus may include:

executing the suspect parent viruses; and

25 determining a suspect parent virus, which generates the child virus after being executed, as the parent virus of the child virus.

[0009] Optionally, the determining virus files, which are first executed within a preset time period before the time when the child virus first appears, as suspect parent viruses may include:

calculating difference between the time when the child virus first appears and the

time when each of the virus files except the child virus in the computer is first executed, to obtain a plurality of differences; and

determining virus files, which correspond to differences in the plurality of differences smaller than the preset time period, as the suspect parent viruses.

- 5 [0010] Optionally, the determining virus files, which correspond to differences in the plurality of differences smaller than the preset time period, as the suspect parent viruses may include:

judging, for each of the plurality of differences, whether the difference is smaller than the preset time period;

- 10 obtaining a time when a virus file is first executed corresponding to the difference, if the difference is smaller than the preset time period;

obtaining the virus file corresponding to the time when the virus file is first executed; and

determining the virus file as the suspect parent virus.

- 15 [0011] A device for searching for a parent virus is further provided. The device includes:

a first determination module, configured to determine an arbitrary virus file as a child virus;

a first obtaining module, configured to obtain a computer containing the child virus;

- 20 a second obtaining module, configured to obtain a time when the child virus first appears in the computer;

a third obtaining module, configured to obtain a time when each of virus files except the child virus in the computer is first executed;

- 25 a second determination module, configured to determine virus files, which are first executed within a preset time period before the time when the child virus first appears, as suspect parent viruses; and

a third determination module, configured to determine, from the suspect parent viruses, the parent virus.

- [0012] Optionally, the device may further include:

a fourth obtaining module, configured to obtain extent of each of the suspect parent

viruses;

a sequencing module, configured to sequence the suspect parent viruses in descending order based on the extent of each of the suspect parent viruses; and

a fifth obtaining module, configured to obtain the first n suspect parent viruses,

5 where n is a preset natural number, and

the third determination module is configured to determine, from the first n suspect parent viruses, the parent virus.

[0013] Optionally, the third determination module may include:

an execution sub-module, configured to execute the suspect parent viruses; and

10 a first determination sub-module, configured to determine a suspect parent virus, which generates the child virus after being executed, as the parent virus of the child virus.

[0014] Optionally, the second determination module may include:

15 a first obtaining sub-module, configured to calculate difference between the time when the child virus first appears and the time when each of the virus files except the child virus in the computer is first executed, to obtain a plurality of differences; and

a second determination sub-module, configured to determine virus files, which correspond to differences in the plurality of differences smaller than the preset time period, as the suspect parent viruses.

[0015] Optionally, the second determination sub-module may include:

20 a judgment unit, configured to judge, for each of the plurality of differences, whether the difference is smaller than the preset time period;

a first obtaining unit, configured to obtain a time when a virus file is first executed corresponding to the difference, if the difference is smaller than the preset time period;

25 a second obtaining unit, configured to obtain the virus file corresponding to the time when the virus file is first executed; and

a second determination unit, configured to determine the virus file as the suspect parent virus.

[0016] According to the embodiments, the child virus is firstly determined, and the computers containing the child virus are obtained; the time when the child virus first appears

in the computers is obtained, and the time when each of virus files except the child virus in the computers is first executed is obtained; the difference between the time when the child virus first appears and the time when each of the virus files is first executed is calculated, and the virus files corresponding to the differences smaller than the preset time period are
5 determined as the suspect parent viruses; and finally the parent virus is determined from the suspect parent viruses. Since the child virus is a virus file generated after executing the parent virus, based on a principle that the time when the parent virus is first executed is earlier than the time when the child virus first appears, the suspect parent viruses are determined, and the parent virus is found from the suspect parent viruses accurately.

10 BRIEF DESCRIPTION OF DRAWINGS

[0017] For explaining technical solutions according to embodiments of the disclosure more clearly, drawings to be used in the description of the embodiments of the disclosure are described briefly below. Apparently, the drawings in the following description are merely some embodiments of the disclosure, and other drawings may be obtained by those skilled in
15 the art based on these drawings without any creative work.

[0018] Figure 1 is a flow chart of a method for searching for a parent virus according to a first embodiment of the disclosure;

[0019] Figure 2 is a flow chart of possible steps further included in the method for searching for the parent virus according to the first embodiment of the disclosure;

20 [0020] Figure 3 is a structure diagram of a device for searching for a parent virus according to a second embodiment of the disclosure; and

[0021] Figure 4 is a schematic structure diagram of a terminal according to the second embodiment of the disclosure.

25 DETAILED DESCRIPTION OF EMBODIMENTS

[0022] Technical solutions of embodiments of the disclosure are described clearly and completely hereinafter in conjunction with drawings of the embodiments of the disclosure.

Apparently, the described embodiments are merely part embodiments of the disclosure. Any other embodiment obtained by those skilled in the art without creative work should fall within the scope of protection of the disclosure.

[0023] First Embodiment

5 [0024] Since a child virus is generated by a parent virus, the time when the child virus first appears is later than the time when the parent virus of the child virus is first executed; the parent virus of the child virus is searched for based on this principle in the disclosure. Compared with the prior art, the parent virus is determined by time relationship, rather than by monitoring the approach with which the parent virus generates the child virus; therefore,
10 the searching accuracy for the parent virus is improved.

[0025] Figure 1 is a flow chart of a method for searching for a parent virus according to the embodiment of the disclosure. The method includes the following steps 101-106.

[0026] Step 101 is, determining an arbitrary virus file as a child virus.

[0027] According to the embodiment, an arbitrary virus file is determined as a child virus
15 before searching for the parent virus.

[0028] In practice, a virus usually exists in a form of file. Concepts of a child virus and a parent virus are conditional. One virus file may be referred to as a child virus and a parent virus at the same time. That is, a virus file may be a file that generates other virus file, thereby being referred to as a parent virus, and may also be a file that is generated by other virus file,
20 thereby being referred to as a child virus. A child virus should be determined before searching for a parent virus, and then the parent virus can be searched for based on the child virus. In addition, different child viruses may be generated by a same parent virus.

[0029] Step 102 is, obtaining a computer containing the child virus.

[0030] According to the embodiment, one or more computer containing the child virus is
25 obtained after the child virus is determined. Since the child virus and the parent virus reside on the same computer, subsequent steps are performed on virus files in the one or more computer containing the child virus.

[0031] Step 103 is, obtaining a time when the child virus first appears in the computer.

[0032] According to the embodiment, the time when the child virus first appears in the

computer is obtained after the child virus is determined.

[0033] Step 104 is, obtaining a time when each of virus files except the child virus in the computer is first executed.

[0034] According to the embodiment, after the child virus is determined, the time when
5 each of the virus files except the child virus in the one or more computer is first executed is obtained. A virus file which is never executed is not the processing object in the embodiment, and is not the parent virus of the child virus determined according to the embodiment.

[0035] It should be noted that, execution order of step 103 and step 104 is not limited in the embodiment. Step 104 may be executed after step 103; or step 103 may be executed after step
10 104; or step 103 and step 104 may be executed simultaneously.

[0036] Step 105 is, determining virus files, which are first executed within a preset time period before the time when the child virus first appears, as suspect parent viruses.

[0037] According to the embodiment, the time period is preset based on experience. After the time when each of the virus files is first executed is obtained, the virus files which are first
15 executed within the preset time period before the time when the child virus first appears are obtained and determined as suspect parent viruses.

[0038] In practice, difference between the time when the child virus first appears and the time when each of the virus files is first executed is calculated; then the virus files corresponding to the differences smaller than the preset time period are determined as the
20 suspect parent viruses.

[0039] Specifically, the determining virus files corresponding to the differences smaller than the preset time period as the suspect parent viruses may include:

[0040] judging, for each of the differences, whether the difference is smaller than the preset time period;

25 [0041] obtaining a time when a virus file is first executed corresponding to the difference, if the difference is smaller than the preset time period;

[0042] obtaining the virus file corresponding to the time when the virus file is first executed; and

[0043] determining the virus file as the suspect parent virus.

[0044] Step 106 is, determining, from the suspect parent viruses, the parent virus.

[0045] According to the embodiment, the parent virus is determined after the suspect parent viruses are determined. In practice, the suspect parent viruses may be executed one by one, and a suspect parent virus which generates the child virus after being executed is determined
5 as the parent virus.

[0046] The child virus may have one parent virus or multiple parent viruses.

[0047] According to the embodiment, the parent virus may be further determined after the suspect parent viruses are determined in the step 105. Figure 2 is referred to, which illustrates a flow chart of possible steps further included in the method according to the embodiment.

10 Steps 201-203 may be performed after step 105 and before step 106.

[0048] Step 201 is, obtaining extent of each of the suspect parent viruses.

[0049] According to the embodiment, computers containing the child virus determined in step 101 are firstly obtained; then the number of computers containing each of the suspect parent viruses is obtained. For example, the computers containing the child virus are obtained,
15 and in these computers, the number of computers containing suspect parent virus X is 200 and the number of computers containing suspect parent virus Y is 500, therefore, the extent of suspect parent virus X is 200 and the extent of suspect parent virus Y is 500, the extent of suspect parent virus Y is greater than the extent of suspect parent virus X. The extent may be considered as the number of computers, and the extent of a suspect parent virus may be
20 considered as the number of computers containing this suspect parent virus.

[0050] Step 202 is, sequencing the suspect parent viruses in descending order based on the extent of each of the suspect parent viruses.

[0051] According to the embodiment, after the extents of the suspect parent viruses are obtained, the suspect parent viruses are sequenced in descending order based on the extents.

25 That is, the suspect parent virus with greater extent is sequenced before the suspect parent virus with smaller extent, and the suspect parent viruses are sequenced in descending order one by one.

[0052] Step 203 is, obtaining the first n suspect parent viruses, where n is a preset natural number.

[0053] According to the embodiment, the natural number n is set based on experience, and the first n suspect parent viruses in the descending sequence are obtained. Since the child virus and the parent virus reside in the same computer, suspect parent virus with greater extent is more likely to be determined as the parent virus. Therefore, the first n suspect parent viruses with greater extents are obtained in this step.

[0054] In practice, step 106 of determining the parent virus from the suspect parent viruses may include step 204.

[0055] Step 204 is, determining the parent virus from the first n suspect parent viruses.

[0056] According to the embodiment, after the first n suspect parent viruses with greater extents are obtained, the parent virus is determined from the first n suspect parent viruses. Specifically, the first n suspect parent viruses are executed one by one; then a suspect parent virus which generates the child virus after being executed is determined as the parent virus of the child virus.

[0057] According to the embodiment, the extents of the suspect parent viruses are obtained, then the suspect parent viruses are sequenced in descending order based on the extents, and the first n suspect parent viruses with greater extents are determined as objects to be executed. Therefore, the number of the virus files to be executed is decreased, and the efficiency of obtaining the parent virus is accordingly improved.

[0058] According to the embodiment, the child virus is firstly determined, and the computers containing the child virus are obtained; the time when the child virus first appears in the computers is obtained, and the time when each of virus files except the child virus in the computers is first executed is obtained; the difference between the time when the child virus first appears and the time when each of the virus files is first executed is calculated, and the virus files corresponding to the differences smaller than the preset time period are determined as the suspect parent viruses; and finally the parent virus is determined from the suspect parent viruses. Since the child virus is a virus file generated after executing the parent virus, based on a principle that the time when the parent virus is first executed is earlier than the time when the child virus first appears, the suspect parent viruses are determined, and the parent virus is found from the suspect parent viruses accurately.

[0059] Second Embodiment

[0060] Figure 3 illustrates a structure diagram of a device for searching for a parent virus according to the embodiment. The device includes a first determination module 301, a first obtaining module 302, a second obtaining module 303, a third obtaining module 304, a
5 second determination module 305 and a third determination module 306.

[0061] The first determination module 301 is configured to determine an arbitrary virus file as a child virus.

[0062] The first obtaining module 302 is configured to obtain a computer containing the child virus.

10 [0063] The second obtaining module 303 is configured to obtain a time when the child virus first appears in the computer.

[0064] The third obtaining module 304 is configured to obtain a time when each of virus files except the child virus in the computer is first executed.

[0065] The second determination module 305 is configured to determine virus files, which
15 are first executed within a preset time period before the time when the child virus first appears, as suspect parent viruses.

[0066] The second determination module 305 may include:

[0067] a first obtaining sub-module, configured to calculate difference between the time when the child virus first appears and the time when each of the virus files except the child
20 virus in the computer is first executed, to obtain a plurality of differences; and

[0068] a second determination sub-module, configured to determine virus files, which correspond to differences in the plurality of differences smaller than the preset time period, as the suspect parent viruses.

[0069] The second determination sub-module may include:

25 [0070] a judgment unit, configured to judge, for each of the plurality of differences, whether the difference is smaller than the preset time period;

[0071] a first obtaining unit, configured to obtain a time when a virus file is first executed corresponding to the difference, if the difference is smaller than the preset time period;

[0072] a second obtaining unit, configured to obtain the virus file corresponding to the time

when the virus file is first executed; and

[0073] a second determination unit, configured to determine the virus file as the suspect parent virus.

[0074] The third determination module 306 is configured to determine, from the suspect parent viruses, the parent virus.

[0075] The third determination module 306 may include:

[0076] an execution sub-module, configured to execute the suspect parent viruses; and

[0077] a first determination sub-module, configured to determine a suspect parent virus, which generates the child virus after being executed, as the parent virus of the child virus.

[0078] To determine the parent virus based on the suspect parent viruses determined by the second determination module 305, the device may further include:

[0079] a fourth obtaining module, configured to obtain extent of each of the suspect parent viruses;

[0080] a sequencing module, configured to sequence the suspect parent viruses in descending order based on the extent of each of the suspect parent viruses; and

[0081] a fifth obtaining module, configured to obtain the first n suspect parent viruses, where n is a preset natural number.

[0082] Correspondingly, the third determination module is configured to determine, from the first n suspect parent viruses, the parent virus.

[0083] A terminal is further provided according to an embodiment of the disclosure, as shown in Figure 4. For convenient illustration, only parts related to the embodiment of the disclosure are shown in Figure 4, and technical details not given may refer to the method embodiment of the disclosure. The terminal may include, for example, a mobile phone, a Tablet Personal Computer, a Personal Digital Assistant (PDA), a Point of Sales (POS) and an on-board computer. Here a case that the terminal is a mobile phone is taken as an example.

[0084] Figure 4 is a block diagram illustrating part structure of a mobile phone related to the terminal according to the embodiment of the disclosure. Referring to Figure 4, the mobile phone includes: a Radio frequency (RF) circuit 410, a memory 420, an input unit 430, a display unit 440, a sensor 450, an audio circuit 460, a Wireless Fidelity (WiFi) module 470, a

processor 480, a power source 490, etc. It should be understood by those skilled in the art that, the structure of the mobile phone shown in Figure 4 is not intended to limit the mobile phone, more or less components than those shown in Figure 4 may be included, some components may be combined or arranged in a different manner.

5 [0085] The components of the mobile phone are described in detail as follows in conjunction with Figure 4.

[0086] The RF circuit 410 may be configured to receive and transmit signals in information receiving and transmitting and telephone communication. Specifically, the RF circuit delivers the received downlink information of the base station to the processor 480 to be processed,
10 and transmits the uplink data to the base station. Generally, the RF circuit includes but not limited to an antenna, at least one amplifier, a transceiver, a coupler, a Low Noise Amplifier (LNA), and a duplexer. In addition, the RF circuit 410 may communicate with other devices via wireless communication and network. The wireless communication may use any communication standard or protocol, including but not limited to Global System of Mobile
15 communication (GSM), General Packet Radio Service (GPRS), Code Division Multiple Access (CDMA), Wideband Code Division Multiple Access (WCDMA), Long Term Evolution (LTE), E-mail, and Short Messaging Service (SMS).

[0087] The memory 420 may be configured to store software programs and modules, and the processor 480 may execute various function applications and data processing of the
20 mobile phone by running the software programs and modules stored in the memory 420. The memory 420 may mainly include a program storage area and a data storage area, where the program storage area may be used to store, for example, the operating system and the application required by at least one function (for example, voice playing function, image playing function), and the data storage area may be used to store, for example, data
25 established according to the use of the terminal (for example, audio data, telephone book). In addition, the memory 420 may include a high-speed random access memory and a nonvolatile memory, such as at least one magnetic disk memory, a flash memory, or other volatile solid-state memory.

[0088] The input unit 430 may be configured to receive input numeric or character

information, and to generate a keyboard signal input related to user setting and function control of the mobile phone 400. In a specific embodiment, the input unit 430 may include a touch control panel 431 and other input device 432. The touch control panel 430 is also referred to as a touch display screen, and may collect a touch operation thereon or thereby (for example, an operation on or around the touch control panel 431 that is made by the user with a finger, a touch pen and any other suitable object or accessory), and drive corresponding connection devices according to a preset procedure. Optionally, the touch control panel 431 may include a touch detection device and a touch controller. The touch detection device detects touch orientation of the user, detects a signal generated by the touch operation, and transmits the signal to the touch controller. The touch controller receives touch information from the touch detection device, converts the touch information into touch coordinates and transmits the touch coordinates to the processor 480. The touch controller is also able to receive a command transmitted from the processor 480 and execute the command. In addition, the touch control panel 431 may be implemented by, for example, a resistive panel, a capacitive panel, an infrared panel and a surface acoustic wave panel. In addition to the touch control panel 431, the input unit 430 may also include other input device 432. Specifically, the other input device 432 may include but not limited to one or more of a physical keyboard, a function key (such as a volume control button, a switch button), a trackball, a mouse and a joystick.

[0089] The display unit 440 is configured to display information input by the user or information provided for the user and various menus of the mobile phone. The display unit 440 may include a display panel 441. Optionally, the display panel 441 may be formed in a form of a Liquid Crystal Display (LCD), an Organic Light-Emitting Diode (OLED) or the like. In addition, the display panel 441 may be covered by the touch control panel 431. When the touch control panel 431 detects a touch operation thereon or thereby, the touch control panel 431 transmits the touch operation to the processor 480 to determine the type of the touch event, and then the processor 480 provides a corresponding visual output on the display panel 441 according to the type of the touch event. Although the touch control panel 431 and the display panel 441 implementing the input and output functions of the mobile phone as two

separate components in Figure 4, the touch control panel 431 and the display panel 441 may be integrated together to implement the input and output functions in other embodiment.

[0090] The mobile phone 400 may further include at least one sensor 450, such as an optical sensor, a motion sensor and other sensors. The optical sensor may include an ambient light sensor and a proximity sensor. The ambient light sensor may adjust the luminance of the display panel 441 according to the intensity of ambient light, and the proximity sensor may close the backlight or the display panel 441 when the terminal is approaching to the ear. As a kind of motion sensor, the gravity acceleration sensor may detect the magnitude of acceleration in multiple directions (usually three-axis directions) and detect the value and direction of the gravity when the sensor is in the stationary state. The acceleration sensor may be applied in, for example, an application of mobile phone pose recognition (for example, switching between landscape and portrait, a correlated game, magnetometer pose calibration), a function about vibration recognition (for example, a pedometer, knocking). Other sensors such as a gyroscope, a barometer, a hygrometer, a thermometer, an infrared sensor, which may be further provided in the mobile phone, are not described herein.

[0091] The audio circuit 460, a loudspeaker 461 and a microphone 462 may provide an audio interface between the user and the mobile phone. The audio circuit 460 may transmit an electric signal, converted from received audio data, to the loudspeaker 461, and a voice signal is converted from the electric signal and then outputted by the loudspeaker 461. The microphone 462 converts captured voice signal into an electric signal, the electric signal is received by the audio circuit 460 and converted into audio data. The audio data is outputted to the processor 480 for processing and then sent to another mobile phone via the RF circuit 410; or the audio data is outputted to the memory 420 for further processing.

[0092] WiFi is a short-range wireless transmission technique. The mobile phone may, for example, send and receive E-mail, browse a webpage and access a streaming media for the user by the WiFi module 470, and provide wireless broadband Internet access for the user. Although the WiFi module 470 is shown in Figure 4, it can be understood that the WiFi module 470 is not necessary for the mobile phone 400, and may be omitted as needed within the scope of the essence of the disclosure.

[0093] The processor 480 is a control center of the mobile phone, which connects various parts of the mobile phone by using various interfaces and wires, and implements various functions and data processing of the mobile phone by running or executing the software programs and/or modules stored in the memory 420 and invoking data stored in the memory 420, thereby monitoring the mobile phone as a whole. Optionally, the processor 480 may include one or more processing units. Preferably, an application processor and a modem processor may be integrated into the processor 480. The application processor is mainly used to process, for example, an operating system, a user interface and an application. The modem processor is mainly used to process wireless communication. It can be understood that, the above modem processor may not be integrated into the processor 480.

[0094] The mobile phone 400 further includes a power supply 490 (such as a battery) for powering various components. Preferably, the power supply may be logically connected with the processor 480 via a power management system, therefore, functions such as charging, discharging and power management are implemented by the power management system.

[0095] Although not shown, the mobile phone 400 may also include other modules such as a camera and a Bluetooth module, which are not described herein.

[0096] Specifically, in the embodiment of the disclosure, in order to achieve various functions, the processor 480 in the terminal may load executable files corresponding to processes of one or more application programs, which are to be executed by the processor 480, into the memory 420 based on the following instructions:

[0097] determining an arbitrary virus file as a child virus;

[0098] obtaining a computer containing the child virus;

[0099] obtaining a time when the child virus first appears in the computer;

[0100] obtaining a time when each of virus files except the child virus in the computer is first executed;

[0101] determining virus files, which are first executed within a preset time period before the time when the child virus first appears, as suspect parent viruses; and

[0102] determining, from the suspect parent viruses, the parent virus.

[0103] Optionally, there are further instructions of, after the determining virus files, which

are first executed within a preset time period before the time when the child virus first appears, as suspect parent viruses, and before the determining, from the suspect parent viruses, the parent virus,

[0104] obtaining extent of each of the suspect parent viruses;

- 5 [0105] sequencing the suspect parent viruses in descending order based on the extent of each of the suspect parent viruses; and

[0106] obtaining the first n suspect parent viruses, where n is a preset natural number, and

[0107] the determining, from the suspect parent viruses, the parent virus includes:

[0108] determining, from the first n suspect parent viruses, the parent virus.

- 10 [0109] Optionally, the determining, from the suspect parent viruses, the parent virus includes:

[0110] executing the suspect parent viruses; and

[0111] determining a suspect parent virus, which generates the child virus after being executed, as the parent virus of the child virus.

- 15 [0112] Optionally, the determining virus files, which are first executed within a preset time period before the time when the child virus first appears, as suspect parent viruses includes:

[0113] calculating difference between the time when the child virus first appears and the time when each of the virus files except the child virus in the computer is first executed, to obtain a plurality of differences; and

- 20 [0114] determining virus files, which correspond to differences in the plurality of differences smaller than the preset time period, as the suspect parent viruses.

[0115] Optionally, the determining virus files, which correspond to differences in the plurality of differences smaller than the preset time period, as the suspect parent viruses includes:

- 25 [0116] judging, for each of the plurality of differences, whether the difference is smaller than the preset time period;

[0117] obtaining a time when a virus file is first executed corresponding to the difference, if the difference is smaller than the preset time period;

[0118] obtaining the virus file corresponding to the time when the virus file is first executed;

and

[0119] determining the virus file as the suspect parent virus.

[0120] According to the embodiment, the child virus is firstly determined, and the computers containing the child virus are obtained; the time when the child virus first appears
5 in the computers is obtained, and the time when each of virus files except the child virus in the computers is first executed is obtained; the difference between the time when the child virus first appears and the time when each of the virus files is first executed is calculated, and the virus files corresponding to the differences smaller than the preset time period are determined as the suspect parent viruses; and finally the parent virus is determined from the
10 suspect parent viruses. Since the child virus is a virus file generated after executing the parent virus, based on a principle that the time when the parent virus is first executed is earlier than the time when the child virus first appears, the suspect parent viruses are determined, and the parent virus is found from the suspect parent viruses accurately.

[0121] Since the device embodiments substantially correspond to the method embodiments,
15 the device embodiments may be implemented by referring to the description of the method embodiments. The device embodiments are described schematically, in which units explained as separated components may be or may not be physically separated, and components shown as units may be or may not be physical units, that is, the components may be located at one place, or distributed on multiple network units. In practice, part or all of the modules may be
20 selected to realize the objective of the embodiment. Those of ordinary skill in the art may understand and implement the disclosure without paying any creative work.

[0122] It should be noted that, relational terms such as first and second herein are just used to distinguish one entity or operation from another entity or operation, which do not necessarily require or indicate that any of such actual relationship or sequence exists between
25 these entities or operations. In addition, terms “comprise”, “include” or any other variation thereof intends to be understood in a non-exclusive sense, so that a process, a method, an object or a device including a series of elements not only include these elements, but also includes other elements not explicitly listed, or further includes elements inherent in the process, the method, the object or the device. In the absence of more restrictions, element

defined by a sentence “includes a...” or “comprises a...” does not exclude that other same elements also exist in the process, the method, the object or the device including said element.

[0123] The method and device for searching for the parent virus according to the embodiments of the disclosure are described in detail hereinabove. The principle and

5 embodiments of the disclosure are illustrated with examples, and the description of the embodiments is adapted to facilitate understanding the method and spirit of the disclosure. Changes may be made on the embodiments and the application scope by those skilled in the art based on the spirit of the disclosure. Accordingly, the contents herein are not intended to limit the disclosure.

WHAT IS CLAIMED IS:

1. A method for searching for a parent virus, comprising:

determining an arbitrary virus file as a child virus;

5 obtaining a computer containing the child virus;

obtaining a time when the child virus first appears in the computer;

obtaining a time when each of virus files except the child virus in the computer is first executed;

10 determining virus files, which are first executed within a preset time period before the time when the child virus first appears, as suspect parent viruses; and

determining, from the suspect parent viruses, the parent virus.

2. The method according to claim 1, wherein the method further comprises, after the determining virus files, which are first executed within a preset time period before the time
15 when the child virus first appears, as suspect parent viruses, and before the determining, from the suspect parent viruses, the parent virus,

obtaining extent of each of the suspect parent viruses;

sequencing the suspect parent viruses in descending order based on the extent of each of the suspect parent viruses; and

20 obtaining the first n suspect parent viruses, wherein n is a preset natural number, and

the determining, from the suspect parent viruses, the parent virus comprises:

determining, from the first n suspect parent viruses, the parent virus.

3. The method according to claim 1, wherein the determining, from the suspect parent
25 viruses, the parent virus comprises:

executing the suspect parent viruses; and

determining a suspect parent virus, which generates the child virus after being executed, as the parent virus of the child virus.

4. The method according to claim 1, wherein the determining virus files, which are first executed within a preset time period before the time when the child virus first appears, as suspect parent viruses comprises:

calculating difference between the time when the child virus first appears and the time when each of the virus files except the child virus in the computer is first executed, to obtain a plurality of differences; and

determining virus files, which correspond to differences in the plurality of differences smaller than the preset time period, as the suspect parent viruses.

5. The method according to claim 4, wherein the determining virus files, which correspond to differences in the plurality of differences smaller than the preset time period, as the suspect parent viruses comprises:

judging, for each of the plurality of differences, whether the difference is smaller than the preset time period;

obtaining a time when a virus file is first executed corresponding to the difference, if the difference is smaller than the preset time period;

obtaining the virus file corresponding to the time when the virus file is first executed; and

determining the virus file as the suspect parent virus.

6. A device for searching for a parent virus, comprising:

a first determination module, configured to determine an arbitrary virus file as a child virus;

a first obtaining module, configured to obtain a computer containing the child virus;

a second obtaining module, configured to obtain a time when the child virus first appears in the computer;

a third obtaining module, configured to obtain a time when each of virus files except the child virus in the computer is first executed;

a second determination module, configured to determine virus files, which are first

executed within a preset time period before the time when the child virus first appears, as suspect parent viruses; and

a third determination module, configured to determine, from the suspect parent viruses, the parent virus.

5

7. The device according to claim 6, wherein the device further comprises:

a fourth obtaining module, configured to obtain extent of each of the suspect parent viruses;

10 a sequencing module, configured to sequence the suspect parent viruses in descending order based on the extent of each of the suspect parent viruses; and

a fifth obtaining module, configured to obtain the first n suspect parent viruses, wherein n is a preset natural number, and

the third determination module is configured to determine, from the first n suspect parent viruses, the parent virus.

15

8. The device according to claim 6, wherein the third determination module comprises:

an execution sub-module, configured to execute the suspect parent viruses; and

a first determination sub-module, configured to determine a suspect parent virus, which generates the child virus after being executed, as the parent virus of the child virus.

20

9. The device according to claim 6, wherein the second determination module comprises:

a first obtaining sub-module, configured to calculate difference between the time when the child virus first appears and the time when each of the virus files except the child virus in the computer is first executed, to obtain a plurality of differences; and

25 a second determination sub-module, configured to determine virus files, which correspond to differences in the plurality of differences smaller than the preset time period, as the suspect parent viruses.

10. The device according to claim 9, wherein the second determination sub-module

comprises:

a judgment unit, configured to judge, for each of the plurality of differences, whether the difference is smaller than the preset time period;

5 a first obtaining unit, configured to obtain a time when a virus file is first executed corresponding to the difference, if the difference is smaller than the preset time period;

a second obtaining unit, configured to obtain the virus file corresponding to the time when the virus file is first executed; and

a second determination unit, configured to determine the virus file as the suspect parent virus.

10

11. A computer-readable medium storing a computer program, wherein execution of the computer program is for:

determining an arbitrary virus file as a child virus;

obtaining a computer containing the child virus;

15 obtaining a time when the child virus first appears in the computer;

obtaining a time when each of virus files except the child virus in the computer is first executed;

determining virus files, which are first executed within a preset time period before the time when the child virus first appears, as suspect parent viruses; and

20 determining, from the suspect parent viruses, the parent virus.

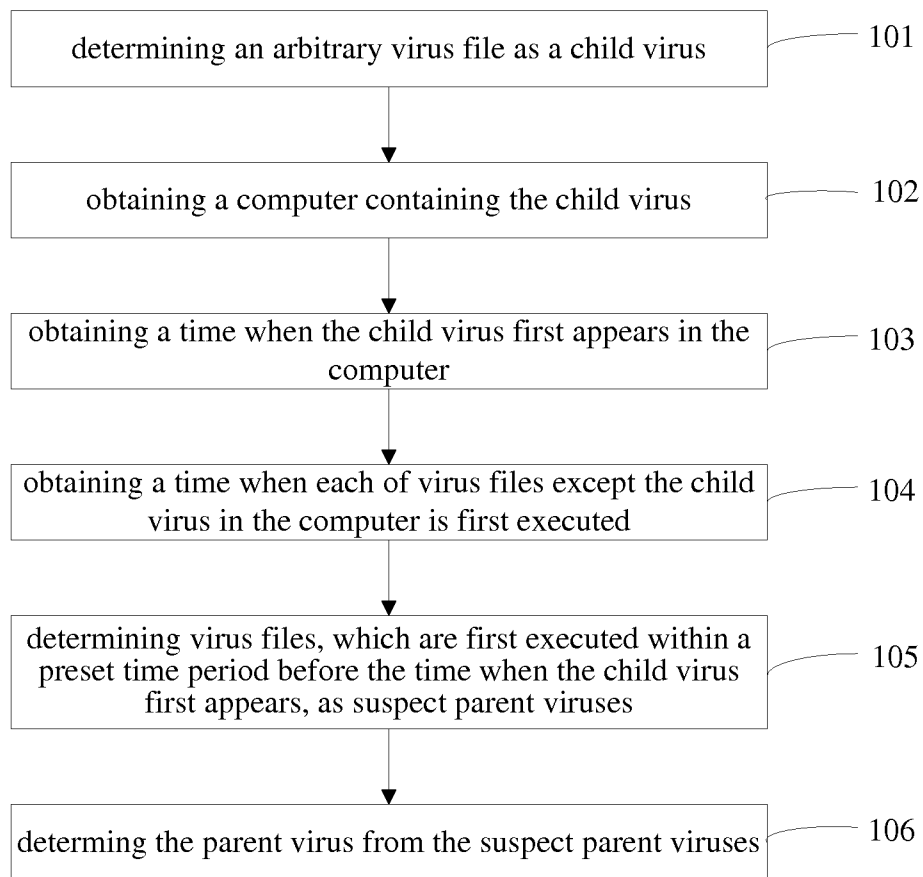


Fig. 1

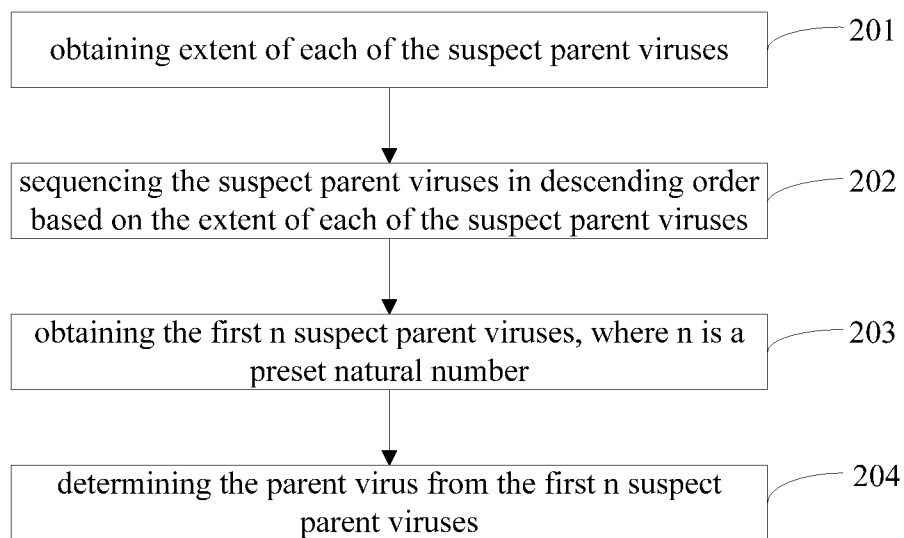


Fig. 2

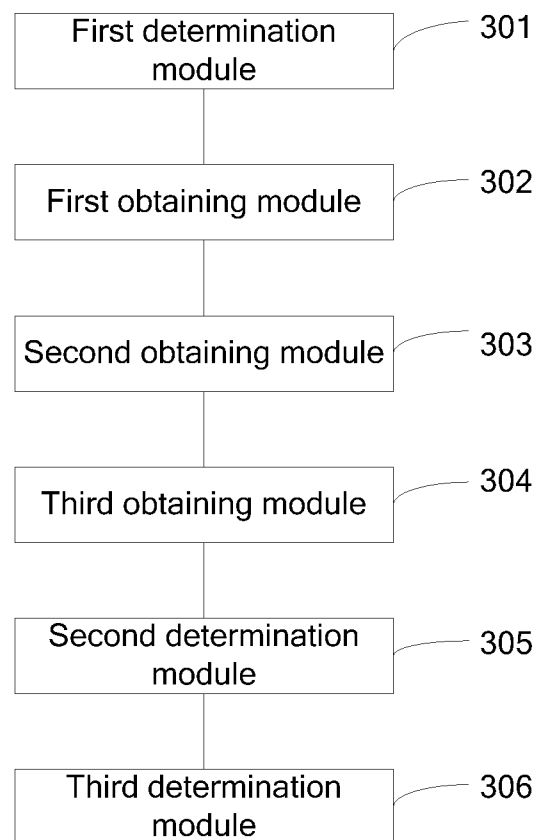


Fig. 3

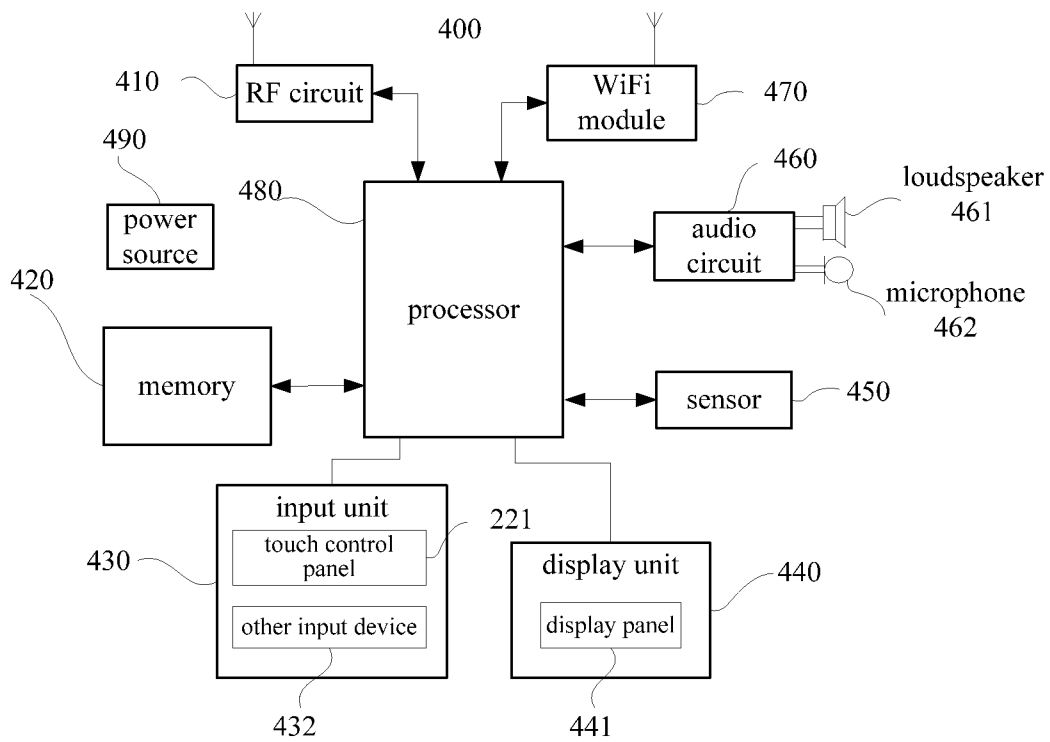


Fig. 4

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2013/090623

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/56 (2013.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: G06F17/-; G06F21/-

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched 0061

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

VEN, CNABS, CNKI, GOOGLE: virus, malware, malicious, file, object, program, code, search???, detect???, identif???, detemin???, locat???, parent, father, child, time, appear

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 103310155 A (TENCENT TECHNOLOGY SHENZHEN CO LTD) 18 September 2013 (18.09.2013) claims 1-10, description paragraphs [0061]-[0116] and [0130]-[0152], figures 1-4	1-11
A	CN 101604361 A (BEIJING QIHOO SCI&TECHNOLOGY CO LTD) 16 December 2009 (16.12.2009) the whole document	1-11
A	US 7472420 B1 (KASPERSKY LAB STOCK CO) 30 December 2008(30.12.2008) the whole document	1-11
A	EP 2584484 A1 (KASPERSKY LAB STOCK CO) 24 April 2013(24.04.2013) the whole document	1-11

☐ Further documents are listed in the continuation of Box C.☒ See patent family annex.

* Special categories of cited documents:	“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
“A” document defining the general state of the art which is not considered to be of particular relevance	“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
“E” earlier application or patent but published on or after the international filing date	“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
“L” document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)	“&”document member of the same patent family
“O” document referring to an oral disclosure, use, exhibition or other means	
“P” document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 23 February 2014 (23.02.2014)	Date of mailing of the international search report 20 Mar. 2014 (20.03.2014)
Name and mailing address of the ISA/CN The State Intellectual Property Office, the P.R.China 6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China 100088 Facsimile No. 86-10-62019451	Authorized officer HAO, Xiaoli Telephone No. (86-10)62089281

International application No.
PCT/CN2013/090623

Form PCT/ISA /210 (patent family annex) (July 2009)