(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 July 2014 (17.07.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/107991 A1

(51) International Patent Classification:
*G06F 21/00* (2013.01)

(21) International Application Number:
PCT/CN2013/087166

(22) International Filing Date:
14 November 2013 (14.11.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
201310008632.8 10 January 2013 (10.01.2013) CN

(71) Applicant: **TENCENT TECHNOLOGY (SHENZHEN) COMPANY LIMITED** [CN/CN]; Room 403, East Block 2, SEG Park, Zhenxing Road, Futian, Shenzhen, Guangdong 518000 (CN).

(72) Inventor: **GUO, Yibin**; Room 403, East Block 2, SEG Park, Zhenxing Road, Futian, Shenzhen, Guangdong 518000 (CN).

(74) Agent: **GUANGZHOU SCIHEAD PATENT AGENT CO., LTD**; Room 1508, Huihua Commercial & Trade Building, No. 80, XianLie Zhong Road, Yuexiu, Guangzhou, Guangdong 510070 (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 ANTI-VIRUS SCANNING

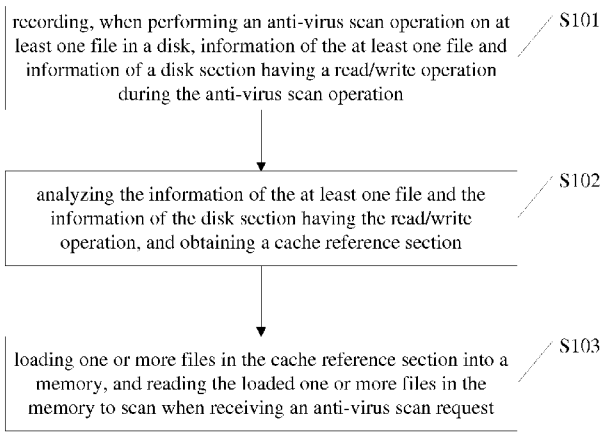


Fig. 1

(57) **Abstract**: A method for anti-virus scanning is described, including: when performing an anti-virus scan operation on at least one file in a disk, recording information of the at least one file and information of a disk section having a read/write operation during the anti-virus scan operation; analyzing the information of the at least one file and the information of the disk section having the read/write operation during the anti-virus scan operation, and obtaining a cache reference section; loading one or more files in the cache reference section into a memory, and reading the loaded one or more files in the memory to scan when receiving an anti-virus scan request. Further, a device for anti-virus scanning is also described. In the method and the device, the amount of disk read/write operations during the anti-virus scan can be decreased, and the efficiency of anti-virus scanning can be improved.

WO 2014/107991 A1

# METHOD AND DEVICE FOR ANTI-VIRUS SCANNING

## CROSS-REFERENCE TO RELATED APPLICATIONS

This application claims the priority benefit of Chinese Patent Application No. 201310008632.8, filed January 10, 2013, the content of which is incorporated by reference herein in its entirety for all purposes.

## FIELD

The disclosure relates to the field of internet technology, and particularly to a method and a device for anti-virus scanning.

## BACKGROUND

As the development and the popularization of the internet, more and more users start to experience the internet. However, not all the environments and the resources of the internet could be secured. If a user terminal is infected by a virus, it may cause terminal system paralysis or hardware damage, even cause the user privacy information leakage to threaten the personal and property safety. Thus, the problem of internet security is increasingly concerned by people. A conventional method of anti-virus includes two parts which are static defense and dynamic defense, and these two parts are the cornerstones for confronting the spread of virus. The static defense therein is an even more fundamental technique in anti-virus process, and some basic functions of dynamic defense also need to be provided and strengthened by the static defense. Moreover, in the static defense, the performance of anti-virus engine is most important. There are several measuring indices for the performance of

anti-virus engine, such as virus detection rate, virus killing rate, efficiency of anti-virus scanning, etc., while one of the critical measuring indices is the efficiency of anti-virus scanning. When performing an anti-virus scanning, the anti-virus engine needs to consider both of disk read/write operations and calculations. Therefore, in a conventional anti-virus engine, the disk read/write operation as a key factor for the efficiency of anti-virus scanning becomes the bottleneck of the conventional anti-virus engine performance.

In a conventional anti-virus method, by caching a to-be-scanned file into a memory and scanning the to-be-scanned file in the memory, the amount of disk read/write operations in a subsequent anti-virus scanning is reduced, and thus, the efficiency of anti-virus scanning is improved. Due to the limited capacity of a memory, this method usually caches only virus files into a memory, while for the huge amount of normal files on a user terminal, there is no definite method to instruct whether and which files need to be cached into the memory. Therefore, the conventional anti-virus method consumes such a long time, and the efficiency of anti-virus scanning is low.

## SUMMARY

Exemplary embodiments of the present invention provide a method and a device for anti-virus scanning, which can reduce the amount of disk read/write operations during the anti-virus scanning and improve the efficiency of anti-virus scanning.

One embodiment of the present invention provides a method for anti-virus scanning, comprising: when performing an anti-virus scan operation on at least one file in a disk, recording information of the at least one file and information of a disk section having

a read/write operation during the anti-virus scan operation; analyzing the information of the at least one file and the information of the disk section having the read/write operation during the anti-virus scan operation, and obtaining a cache reference section; loading one or more files in the cache reference section into a memory, and reading the loaded one or more files in the memory to scan when receiving an anti-virus scan request.

Another embodiment of the present invention provides a device for anti-virus scanning, comprising: an anti-virus scanning unit, which is configured to perform an anti-virus scan operation on at least one file in a disk; a recording unit, which is configured to when performing an anti-virus scan operation on at least one file in a disk, record information of the at least one file and information of a disk section having a read/write operation during the anti-virus scan operation; a processing unit, which is configured to analyze the information of the at least one file and the information of the disk section having the read/write operation during the anti-virus scan operation and obtain a cache reference section; and a caching unit, which is configured to load one or more files in the cache reference section into a memory, and indicate the anti-virus scanning unit to read the loaded one or more files from the memory to scan when the anti-virus scanning unit receives an anti-virus scan request.

Exemplary embodiments of the present invention may have the following benefit effects.

A cache reference section can be obtained by recording and analyzing information of at least one file and information of a disk section having a read/write operation during an anti-virus scan operation on the at least one file. So, when scanning next time, one or more files in the cache reference section can be pre-loaded into a memory.

Thus, cache data can be identified, and the efficiency of anti-virus scanning can be improved. By classifying files to select proper cache files according to file popularity, a reading attribute of anti-virus engine, and unhitted cache data reported by a terminal, the range of cache reference section can be compressed, and the hit rate of cache files can be raised. Moreover, by judging whether the file capacity of cache reference section is appropriate so as to compress the cache reference section repeatedly, the memory storage pressure can be reduced, and the efficiency of anti-virus scanning can be increased without affecting the process performance. When a cache file is unhitted, the section corresponding to the unhitted cache file may be combined into the cache reference section. Therefore, the cache reference section can be further improved, and the hit rate of cache files can be enhanced.

## BRIEF DESCRIPTION OF THE DRAWINGS

In order to illustrate the embodiments or existing technical solutions more clearly, a brief description of drawings that assists the description of embodiments of the invention or existing art will be provided below. It would be apparent that the drawings in the following description are only for some of the embodiments of the invention. A person having ordinary skills in the art will be able to obtain other drawings on the basis of these drawings without paying any creative work.

Fig. 1 is a flowchart of a method for anti-virus scanning according to one embodiment of the invention;

Fig. 2 is a flowchart of a method for anti-virus scanning according to another embodiment of the invention;

Fig. 3 is a flowchart of a method for anti-virus scanning according to yet another

embodiment of the invention;

Fig. 4 is a flowchart of a method for anti-virus scanning according to yet another embodiment of the invention;

Fig. 5 is a structure diagram of a device for anti-virus scanning according to yet another embodiment of the invention;

Fig. 6 is a structure diagram of a device for anti-virus scanning according to yet another embodiment of the invention;

Fig. 7 is a structure diagram of a device for anti-virus scanning according to yet another embodiment of the invention;

Fig. 8 is a structure diagram of a device for anti-virus scanning according to yet another embodiment of the invention.

## DETAILED DESCRIPTION

Technical solutions in embodiments of the present invention will be illustrated clearly and entirely with the aid of the drawings in the embodiments of the invention. It is apparent that the illustrated embodiments are only some embodiments of the invention instead of all of them. Other embodiments that a person having ordinary skills in the art obtains based on the illustrated embodiments of the invention without paying any creative work should all be within the protection scope sought by the present invention.

Referring to Fig. 1, it is a flowchart of a method for anti-virus scanning according to one embodiment of the invention. The method comprises the following steps.

Step S101 is: when performing an anti-virus scan operation on at least one file in a disk, recording information of the at least one file and information of a disk section

having a read/write operation during the anti-virus scan operation.

Specifically, information of each of the at least one file comprises: a file type, and a hash data of the file; wherein, the file type is used to classify files and perform statistic on disk sections having read/write operations for files of respective types; and the hash data of the file is used to check correction and integration of the file.

It is obvious that information of each of the at least one file can further comprise but not limited to other information of file attributes, such as the version number, shelled or unshelled, compressed or uncompressed, etc.

Step S102 is: analyzing the information of the at least one file and the information of the disk section having the read/write operation, and obtaining a cache reference section.

Step S103 is: loading one or more files in the cache reference section into a memory, and reading the loaded one or more files in the memory to scan when receiving an anti-virus scan request.

By recording and analyzing information of the at least one file and information of disk section having a read/write operation during scanning the at least one file, a cache reference section is obtained. So, when scanning next time, the at least one file in the cache reference section can be pre-loaded into a memory. Thus, cache data can be identified, and the efficiency of anti-virus scanning can be improved.

Referring to Fig. 2, it is a flowchart of a method for anti-virus scanning according to another embodiment of the invention. The method comprises the following steps.

Step S201 is: recording, when performing an anti-virus scan operation on at least one file in a disk, information of the at least one file and information of a disk section having a read/write operation.

Step S202 is: classifying all files according to their file types.

Generally, for files of different types, disk sections that have read/write operations are normally different. For example, the disk section having a read/write operation for a picture file apparently differs from the one for a compressed file. If performing the same operation on files of different types, it would affect the correction of subsequent analysis and calculations on the cache reference section.

Step S203 is: for files of different types, selecting cache files according to at least one of file popularity, a reading attribute of anti-virus engine, and unhitted cache data reported by a terminal.

Specifically, the file popularity is high when a file is frequently used, and the file popularity is low when a file is rarely used. For a file with high file popularity, its corresponding disk section having read/write operations usually needs to be preferentially considered, while for a file with low file popularity, it may not be necessary to be added into cache. Particularly, when there is confliction between the disk section having a read/write operation of high-popularity file and the one of low-popularity file, the high-popularity file should have priority to be admissible. Generally, a popularity threshold may be preset to indicate the frequency of use for a file in a preset duration. When its file popularity reaches the popularity threshold, a file will be judged as a high-popularity file.

The reading attribute of an anti-virus engine may be frequencies of the anti-virus engine reading respective sections of the disk. For example, some anti-virus engine will frequently read a certain section in a disk, and thus, the data in this section can be added into the cache reference section.

For the data not included in the cache reference section, its corresponding section can

also be added into the cache reference section when reported by a terminal.

After screened by one or more of the screening criteria described above, a series of disk sections having read/write operations can be obtained.

Step S204 is: combining disk sections having read/write operations corresponding to the cache files to obtain the cache reference section.

Step S205 is: loading one or more files in the cache reference section into a memory, and reading the loaded one or more files in the memory to scan when receiving an anti-virus scan request.

By the analyzing method described above in one embodiment, disk sections having read/write operations corresponding to frequently used files can be obtained. A cache reference section obtained by combining these sections can have a relatively high hit rate. As a result, the efficiency of anti-virus scanning can be relatively improved while the storage pressure of memory can be decreased.

Referring to Fig. 3, it is a flowchart of a method for anti-virus scanning according to yet another embodiment of the invention. The method comprises the following steps.

Step S301is: recording, when performing an anti-virus scan operation on at least one file in a disk, information of the at least one file and information of a disk section having a read/write operation.

Step S302 is: classifying all files according to their file types.

Step S303 is: for files with different types, selecting cache files according to at least one of file popularity, a reading attribute of anti-virus engine, and unhitted cache data reported by a terminal.

Step S304 is: combining disk sections having read/write operations corresponding to

the cache files to obtain the cache reference section.

Step S305 is: judging whether a file capacity in the cache reference section exceeds a preset threshold.

Generally, the storage capacity of a memory is limited. If too many files are cached, the performance of processing unit would be decreased, and thus processing fluency of the anti-virus scanning would be influenced. Therefore, it is very important for efficiency control of anti-virus scanning to introduce reasonable judgment mechanism to control the size of cache reference section.

Step S306 is: performing an anti-virus scan operation on files in the cache reference section, recording information of the files and information of disk sections having read/write operations during the anti-virus scan operation, analyzing the information of the files and the information of the disk sections having the read/write operations during the anti-virus scan operation, until the file capacity in the cache reference section meets the requirement of the preset threshold.

Herein, a method for further compressing the cache reference section is provided. By performing continuous cycle of scanning, recording, and analyzing on the files in the cache reference section, a more appropriate cache reference section can be obtained, until the file capacity in the cache reference section meets the requirement of a preset threshold. In this way, the efficiency of anti-virus scanning can be improved without influencing the whole performance of system.

Step S307 is: loading one or more files in the cache reference section into a memory, and reading the loaded one or more files in the memory to scan when receiving an anti-virus scan request.

Referring to Fig. 4, it is a flowchart of a method for anti-virus scanning according to

yet another embodiment of the invention. The method comprises the following steps.

Step S401 is: recording, when performing an anti-virus scan operation on at least one file in a disk, information of the at least one file and information of a disk section having a read/write operation.

Step S402 is: classifying all files according to their file types.

Step S403 is: for files with different types, selecting cache files according to at least one of file popularity, a reading attribute of anti-virus engine, and unhitted cache data reported by a terminal.

Step S404 is: combining disk sections having read/write operations corresponding to the cache files to obtain the cache reference section.

Step S405 is: judging whether a file capacity in the cache reference section exceeds a preset threshold.

Step S406 is: performing an anti-virus scan operation on files in the cache reference section, recording information of the files and information of disk sections having read/write operations during the anti-virus scan operation, analyzing the information of the files and the information of the disk sections having the read/write operations during the anti-virus scan operation, until the file capacity in the cache reference section meets the requirement of the preset threshold.

Step 407 is: loading one or more files in the cache reference section into the memory, and judging whether there exists a to-be-scanned file in the memory when receiving the anti-virus scan request.

Step 408 is: reading the to-be-scanned file directly from the disk to scan, recording information of the to-be-scanned file and information of a disk section having a

read/write operation during the scan on the to-be-scanned file, and combining the disk section having the read/write operation during the scan on the to-be-scanned file into the cache reference section.

The hit rate is greatly improved by the method described before, however, it still cannot exclude that there exists unhitted files in the cache reference section. Accordingly, the cache reference section can be further improved by judging whether there exists a to-be-scanned file; if there exists no to-be-scanned files, reading the to-be-scanned file directly from the disk and performing an anti-virus scan operation, and meanwhile, introducing a parallel adding manner to combine the disk section having a read/write operation which corresponds to the unhitted file into the cache reference section. If the file capacity in the cache reference section exceeds the preset threshold, some rarely used files in the cache reference section may be deleted according to the file type, the file popularity, and the reading attributes of anti-virus engine as references, so as to keep the section size appropriate.

Step S409 is: reading directly from the memory and performing an anti-virus scan operation.

Referring to Fig. 5, it is a structure diagram of a device for anti-virus scanning according to yet another embodiment of the invention. The device comprises: an anti-virus scanning unit 100, a recording unit 200, a processing unit 300 and a caching unit 400.

The anti-virus scanning unit 100 is configured to perform an anti-virus scan operation on at least one file in a disk; the recording unit 200 is configured to when the anti-virus scanning unit 100 performs an anti-virus scan operation on at least one file in a disk, record information of the at least one file and information of a disk section

having a read/write operation during the anti-virus scan operation; the processing unit 300 is configured to analyze the information of the at least one file and the information of the disk section having the read/write operation and obtain a cache reference section; and the caching unit 400 is configured to load one or more files in the cache reference section into a memory, and read the loaded one or more files in the memory to scan when receiving an anti-virus scan request.

Referring to Fig. 6, it is a structure diagram of a device for anti-virus scanning according to yet another embodiment of the invention. The device comprises: an anti-virus scanning unit 100, a recording unit 200, a processing unit 300 and a caching unit 400.

The processing unit 300 comprises: a classifying sub-unit 310, a selecting sub-unit 320, a combining sub-unit 330.

The classifying sub-unit 310 is configured to classify all files according to their file types; the selecting sub-unit 320 is configured to for files with different types, select cache files according to at least one of file popularity, a reading attributes of anti-virus engine, and unhitted cache data reported by a terminal; the combining sub-unit 330 is configured to combine disk sections having read/write operations corresponding to the cache files to obtain a cache reference section, wherein, the file popularity is high if the file is frequently used, and the file popularity is low if the file is rarely used. The reading attributes of anti-virus engine may be frequencies of the anti-virus engine reading respective sections of the disk.

Referring to Fig. 7, it is a structure diagram of a device for anti-virus scanning according to yet another embodiment of the invention. The device comprises: a anti-virus scanning unit 100, a recording unit 200, a processing unit 300, a caching

unit 400 and a first judging unit 500.

The first judging unit 500 is configured to judge whether a file capacity in the cache reference section exceeds a preset threshold, after the combining sub-unit 330 combines disk sections having read/write operations corresponding to the cache files to obtain a cache reference section. If the file capacity exceeds the preset threshold, then it indicates the anti-virus scanning unit 100 to perform an anti-virus scan operation on at least one file in the cache reference section, indicates the recording unit 200 to record information of the at least one file and information of a disk section having a read/write operation during an anti-virus scan operation on the at least one file, and indicates the processing unit 300 to analyze the information of the at least one file and the information of the disk section having the read/write operation during an anti-virus scan operation on the at least one file, until the file capacity in the cache reference section meets the requirement of the preset threshold.

Referring to Fig. 8, it is a structure diagram of a device for anti-virus scanning according to yet another embodiment of the invention. The device comprises: an anti-virus scanning unit 100, a recording unit 200, a processing unit 300, a caching unit 400, a first judging unit 500, and a second judging unit 600.

The second judging unit 600 is configured to load one or more files in the cache reference section into the memory, and judge whether there exists a to-be-scanned file in the memory when the anti-virus scanning unit 100 receives an anti-virus scan request. If there exists no to-be-scanned files, then it indicates the anti-virus scanning unit 100 to directly read the to-be-scanned file from a disk to scan, indicates the recording unit 200 to record information of the to-be-scanned file and information of a disk section having a read/write operation during the scan on the to-be-scanned

file, and indicates the processing unit 300 to combine the disk section having the read/write operation during the scan on the to-be-scanned file into the cache reference section.

It should be noted that various embodiments herein may be described in a progressive manner. One embodiment may be described by emphasizing its difference from other embodiments. For similar/same things between one embodiment and another embodiment, one may refer to the another embodiment. Exemplary embodiments of device may be described briefly here since exemplary embodiments of devices are similar with exemplary embodiments of methods, and for relative things between them, one may refer to the illustrations in the exemplary embodiments of methods.

Based on the above description of embodiments, exemplary embodiments of the present invention may have the following benefits.

A cache reference section is obtained by recording and analyzing information of at least one file and information of a disk section having a read/write operation during anti-virus scan operation on the at least one file. So, when scanning next time, the at least one file in the cache reference section can be pre-loaded into a memory. Thus, cache data can be identified, and the efficiency of anti-virus scanning can be improved. By classifying the files to select proper cache files according to file popularity, a reading attributes of anti-virus engine, and unhitted cache data reported by a terminal, the range of cache reference section can be compressed, and the hit rate of cache files can be raised. Moreover, by judging whether the file capacity of cache reference section is appropriate so as to compress the cache reference section repeatedly, the memory storage pressure can be reduced, and the efficiency of anti-virus scanning can be increased without affecting the process performance. When a cache file is

unhitted, the section corresponding to the unhitted cache file may be combined into the cache reference section. Therefore, the cache reference section can be further improved, and the hit rate of cache files can be enhanced.

A person having ordinary skills in the art can realize that part or whole of the processes in the methods according to the above embodiments may be implemented by a computer program instructing relevant hardware. The program may be stored in a computer readable storage medium. When executed, the program may execute processes in the above-mentioned embodiments of methods. The storage medium may be a magnetic disk, an optical disk, a Read-Only Memory (ROM), a Random Access Memory (RAM), et al.

The above descriptions are some exemplary embodiments of the invention, and should not be regarded as limitation to the scope of related claims. A person having ordinary skills in a relevant technical field will be able to make improvements and modifications within the spirit of the principle of the invention. The improvements and modifications should also be incorporated in the scope of the claims attached below.

# CLAIMS

1. A method for anti-virus scanning, comprising:

recording, when performing an anti-virus scan operation on at least one file in a disk, information of the at least one file and information of a disk section having a read/write operation during the anti-virus scan operation;

analyzing the information of the at least one file and the information of the disk section having the read/write operation, and obtaining a cache reference section;

loading one or more files in the cache reference section into a memory, and reading the loaded one or more files in the memory to scan when receiving an anti-virus scan request.

2. The method of claim 1, wherein information of each of the at least one file comprises:

a file type, and a hash data of the file, wherein:

the file type is used to classify files and perform statistic on disk sections having read/write operations for files of respective types; and

the hash data of the file is used to check correction and integration of the file.

3. The method of claim 2, wherein analyzing the information of the at least one file and the information of the disk section having the read/write operation during the anti-virus scan operation, and obtaining a cache reference section, comprises:

classifying all files according to their file types;

for files with different types, selecting cache files according to at least one of file popularity, a reading attribute of anti-virus engine, and unhitted cache data reported

by a terminal; and

combining disk sections having read/write operations corresponding to the cache files to obtain the cache reference section,

wherein, the file popularity is high when the file is frequently used, and the file popularity is low when the file is rarely used; and the reading attribute of anti-virus engine is frequencies of an anti-virus engine reading respective sections of the disk.

4. The method of claim 3, after combining the disk sections having the read/write operations corresponding to the cache files to obtain the cache reference section, further comprising:

judging whether a file capacity in the cache reference section exceeds a preset threshold; and

if the file capacity exceeds the preset threshold, performing an anti-virus scan operation on files in the cache reference section, recording information of the files and information of disk sections having read/write operations during the anti-virus scan operation, analyzing the information of the files and the information of the disk sections having the read/write operations during the anti-virus scan operation, until the file capacity in the cache reference section meets the requirement of the preset threshold.

5. The method of any one of claims 1 to 4, wherein the step of loading one or more files in the cache reference section into a memory and reading the loaded one or more files in the memory to scan when receiving the anti-virus scan request, comprises:

loading one or more files in the cache reference section into the memory, and

judging whether there exists a to-be-scanned file in the memory when receiving the anti-virus scan request; and

if there exists no to-be-scanned file, reading the to-be-scanned file directly from the disk to scan, recording information of the to-be-scanned file and information of a disk section having a read/write operation during the scan on the to-be-scanned file, and combining the disk section having the read/write operation during the scan on the to-be-scanned file into the cache reference section.

6. A device for anti-virus scanning, comprising:

an anti-virus scanning unit, configured to perform an anti-virus scan operation on at least one file in a disk;

a recording unit, configured to record, when performing an anti-virus scan operation on at least one file in a disk, information of the at least one file and information of a disk section having a read/write operation during the anti-virus scan operation;

a processing unit, configured to analyze the information of the at least one file and the information of the disk section having the read/write operation and obtain a cache reference section;

a caching unit, configured to load one or more files in the cache reference section into a memory, and indicate the anti-virus scanning unit to read the loaded one or more files from the memory to scan when the anti-virus scanning unit receives an anti-virus scan request.

7. The device of claim 6, wherein information of each of the at least one file

comprises:

a file type, and a hash data of the file, wherein:

the file type is used to classify files and perform statistic on disk sections having read/write operations for files of respective types; and

the hash data of the file is used to check correction and integration of the file.

8. The device of claim 7, wherein the processing unit comprises:

a classifying sub-unit, configured to classify all files according to their file types;

a selecting sub-unit, configured to, for files with different types, select cache files according to at least one of file popularity, a reading attribute of anti-virus engine, and unhitted cache data reported by a terminal;

a combining sub-unit, configured to combine disk sections having read/write operations corresponding to the cache files to obtain a cache reference section,

wherein, the file popularity is high when the file is frequently used, and the file popularity is low when the file is rarely used; and the reading attribute of anti-virus engine is frequencies of an anti-virus engine reading respective sections of a disk.

9. The device of claim 8, further comprising:

a first judging unit, configured to judge whether a file capacity in the cache reference section exceeds a preset threshold after the combining sub-unit combines disk sections having read/write operations corresponding to cache files to obtain a cache reference section, wherein

the first judging unit further configured to, if the file capacity exceeds the preset threshold, indicate the anti-virus scanning unit to perform an anti-virus scan operation

on files in the cache reference section, indicate the recording unit to record information of the files and information of disk sections having a read/write operation during an anti-virus scan operation on the files, and indicate the processing unit to analyze the information of the files and the information of the disk sections having the read/write operation during an anti-virus scan operation on the files until the file capacity in the cache reference section meets the requirement of the preset threshold.

10. The device of any one of claims 6 to 9, further comprising:

a second judging unit configured to load one or more files in the cache reference section into the memory, and judge whether there exists a to-be-scanned file in the memory when the anti-virus scanning unit receives an anti-virus scan request, wherein

the second judging unit further configured to, if there exists no to-be-scanned file, indicate the anti-virus scanning unit to directly read the to-be-scanned file from a disk to scan, indicate the recording unit to record information of the to-be-scanned file and information of a disk section having a read/write operation during the scan on the to-be-scanned file, and indicate the processing unit to combine the disk section having the read/write operation during the scan on the to-be-scanned file into the cache reference section.

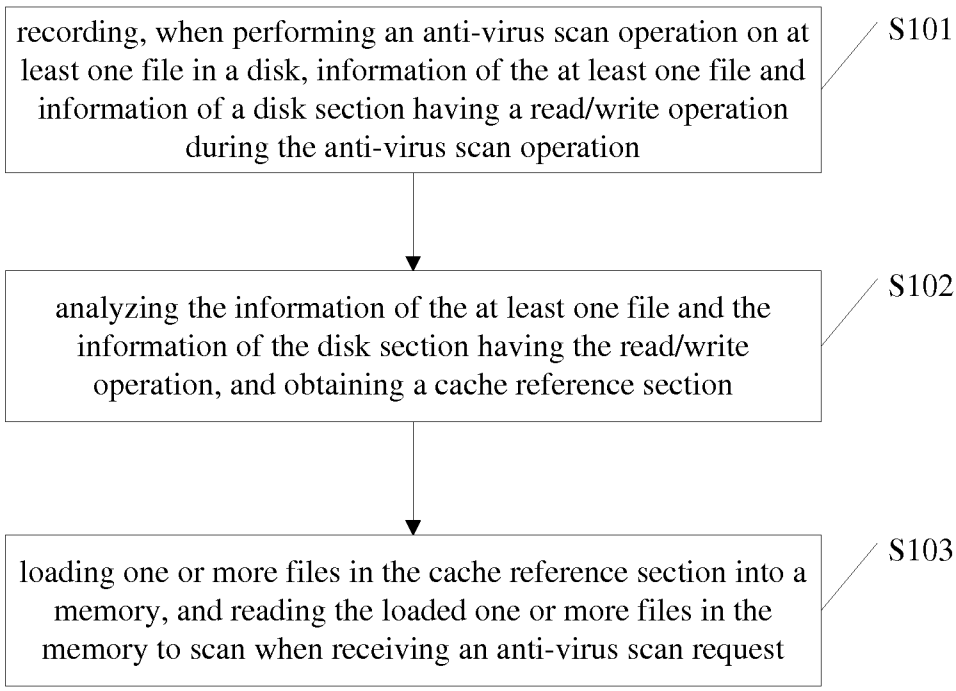
recording, when performing an anti-virus scan operation on at least one file in a disk, information of the at least one file and information of a disk section having a read/write operation during the anti-virus scan operation
S101
analyzing the information of the at least one file and the information of the disk section having the read/write operation, and obtaining a cache reference section
S102
loading one or more files in the cache reference section into a memory, and reading the loaded one or more files in the memory to scan when receiving an anti-virus scan request
S103

Fig. 1

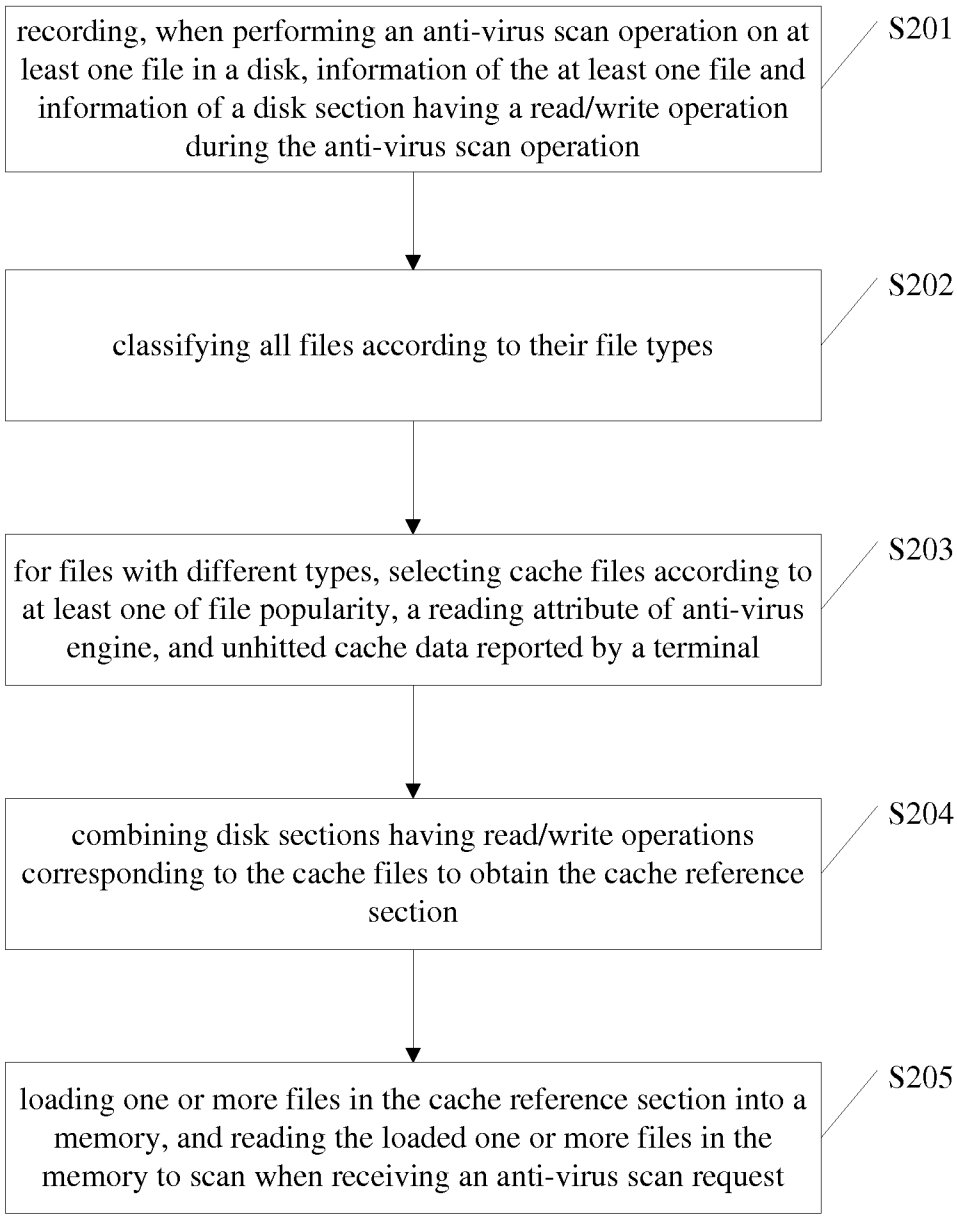
recording, when performing an anti-virus scan operation on at least one file in a disk, information of the at least one file and information of a disk section having a read/write operation during the anti-virus scan operation
S201
classifying all files according to their file types
S202
for files with different types, selecting cache files according to at least one of file popularity, a reading attribute of anti-virus engine, and unhitted cache data reported by a terminal
S203
combining disk sections having read/write operations corresponding to the cache files to obtain the cache reference section
S204
loading one or more files in the cache reference section into a memory, and reading the loaded one or more files in the memory to scan when receiving an anti-virus scan request
S205

Fig. 2

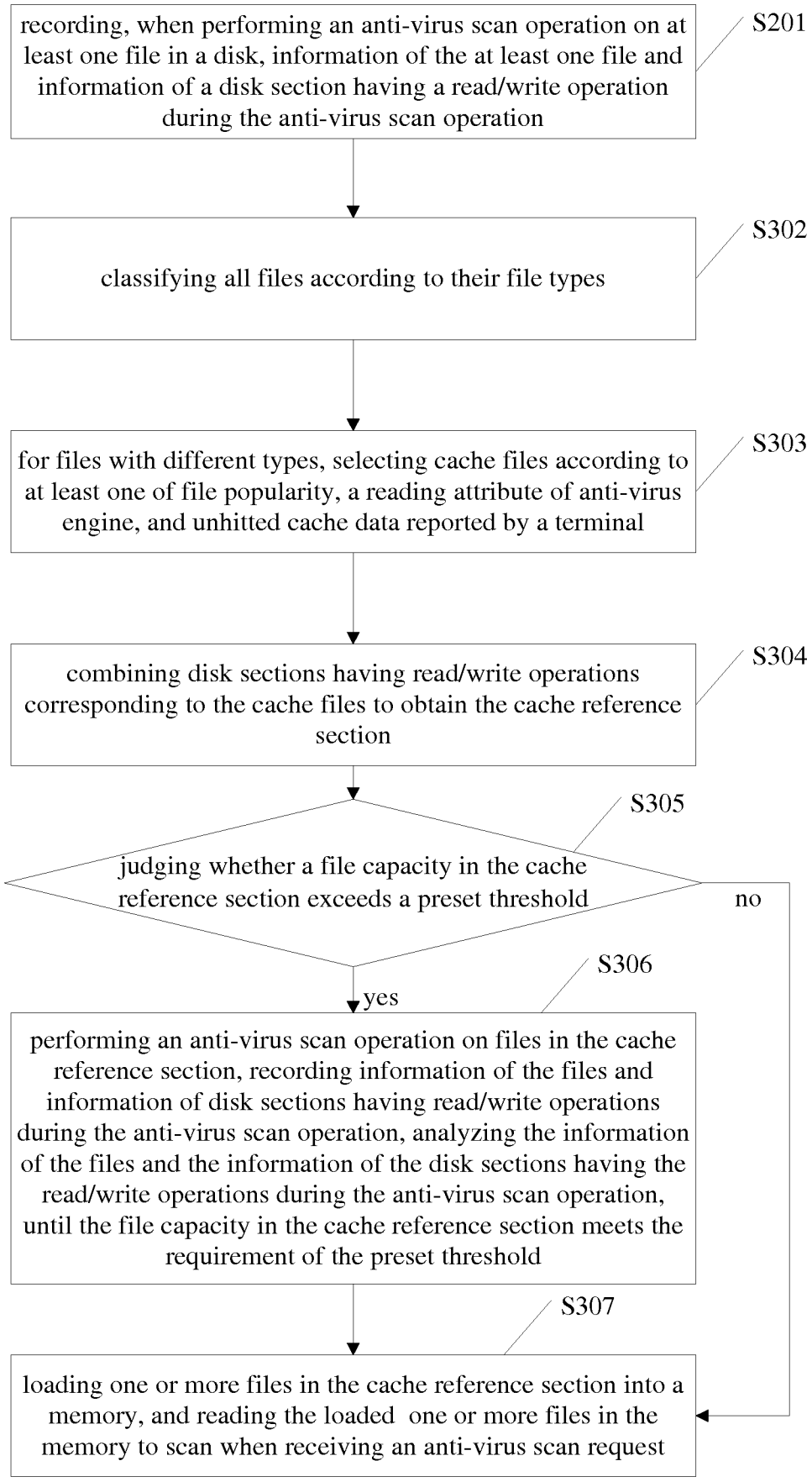
recording, when performing an anti-virus scan operation on at least one file in a disk, information of the at least one file and information of a disk section having a read/write operation during the anti-virus scan operation
S201
classifying all files according to their file types
S302
for files with different types, selecting cache files according to at least one of file popularity, a reading attribute of anti-virus engine, and unhitted cache data reported by a terminal
S303
combining disk sections having read/write operations corresponding to the cache files to obtain the cache reference section
S304
judging whether a file capacity in the cache reference section exceeds a preset threshold
S305
no
yes
S306
performing an anti-virus scan operation on files in the cache reference section, recording information of the files and information of disk sections having read/write operations during the anti-virus scan operation, analyzing the information of the files and the information of the disk sections having the read/write operations during the anti-virus scan operation, until the file capacity in the cache reference section meets the requirement of the preset threshold
S307
loading one or more files in the cache reference section into a memory, and reading the loaded one or more files in the memory to scan when receiving an anti-virus scan request

Fig. 3

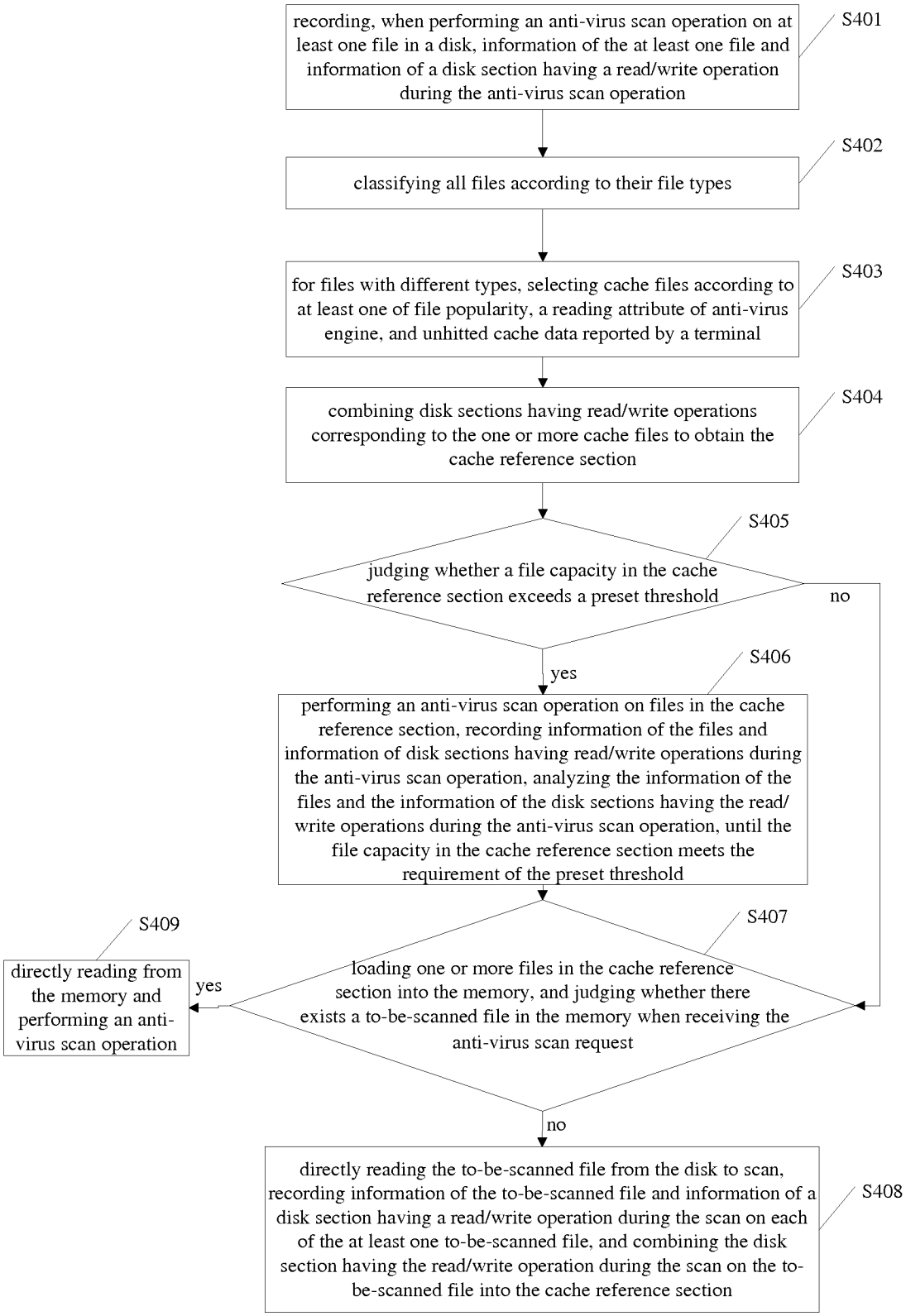
recording, when performing an anti-virus scan operation on at least one file in a disk, information of the at least one file and information of a disk section having a read/write operation during the anti-virus scan operation
S401
classifying all files according to their file types
S402
for files with different types, selecting cache files according to at least one of file popularity, a reading attribute of anti-virus engine, and unhitted cache data reported by a terminal
S403
combining disk sections having read/write operations corresponding to the one or more cache files to obtain the cache reference section
S404
judging whether a file capacity in the cache reference section exceeds a preset threshold
S405
no
yes
performing an anti-virus scan operation on files in the cache reference section, recording information of the files and information of disk sections having read/write operations during the anti-virus scan operation, analyzing the information of the files and the information of the disk sections having the read/write operations during the anti-virus scan operation, until the file capacity in the cache reference section meets the requirement of the preset threshold
S406
loading one or more files in the cache reference section into the memory, and judging whether there exists a to-be-scanned file in the memory when receiving the anti-virus scan request
S407
yes
directly reading from the memory and performing an anti-virus scan operation
S409
no
directly reading the to-be-scanned file from the disk to scan, recording information of the to-be-scanned file and information of a disk section having a read/write operation during the scan on each of the at least one to-be-scanned file, and combining the disk section having the read/write operation during the scan on the to-be-scanned file into the cache reference section
S408

Fig. 4

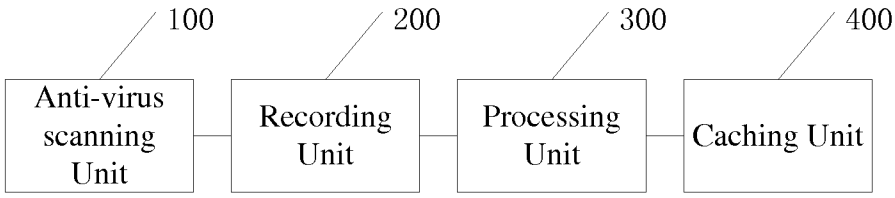
100
200
300
400
Anti-virus scanning Unit
Recording Unit
Processing Unit
Caching Unit

Fig. 5

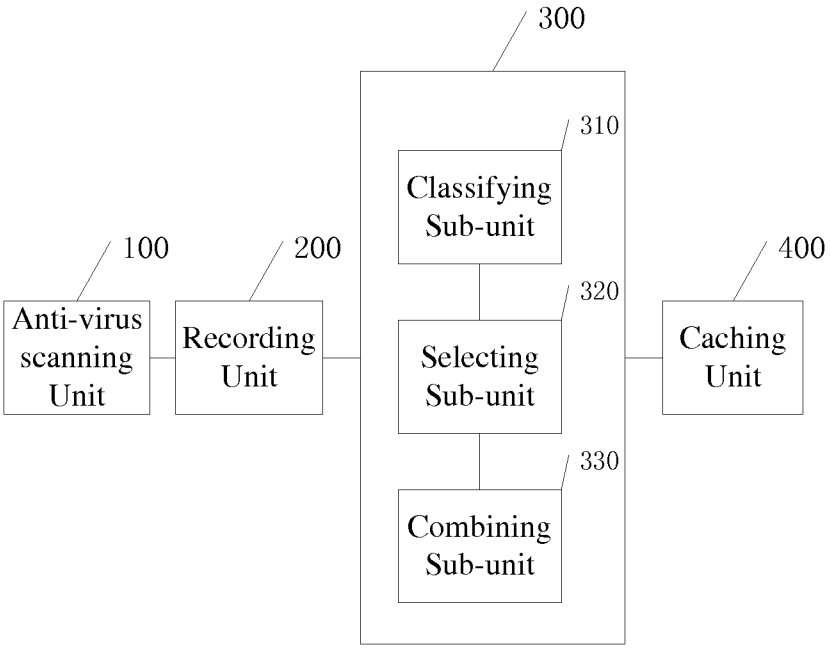
300
310
Classifying Sub-unit
100
200
400
320
Anti-virus scanning Unit
Recording Unit
Selecting Sub-unit
Caching Unit
330
Combining Sub-unit

Fig. 6

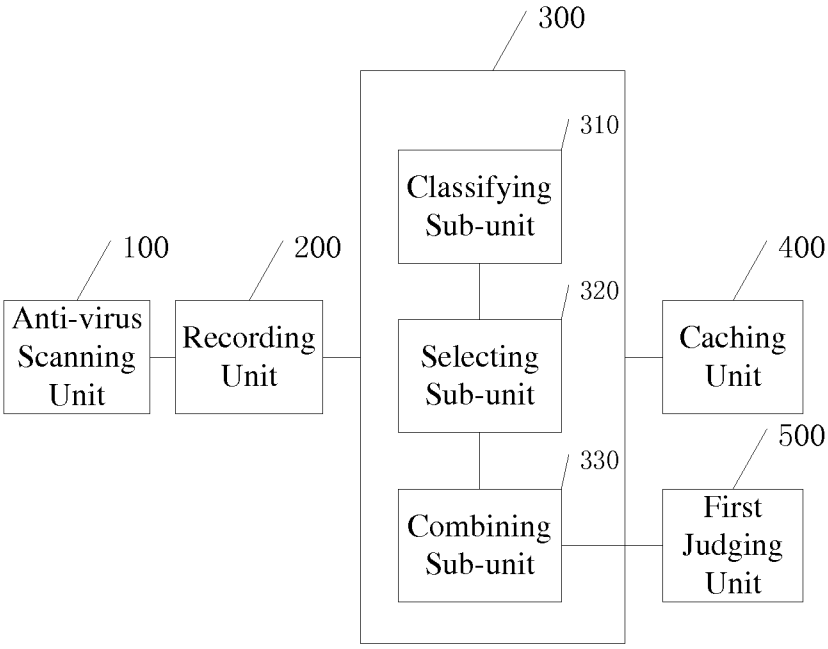
300
310
Classifying Sub-unit
100
200
400
320
Anti-virus Scanning Unit
Recording Unit
Selecting Sub-unit
Caching Unit
500
330
Combining Sub-unit
First Judging Unit

Fig. 7

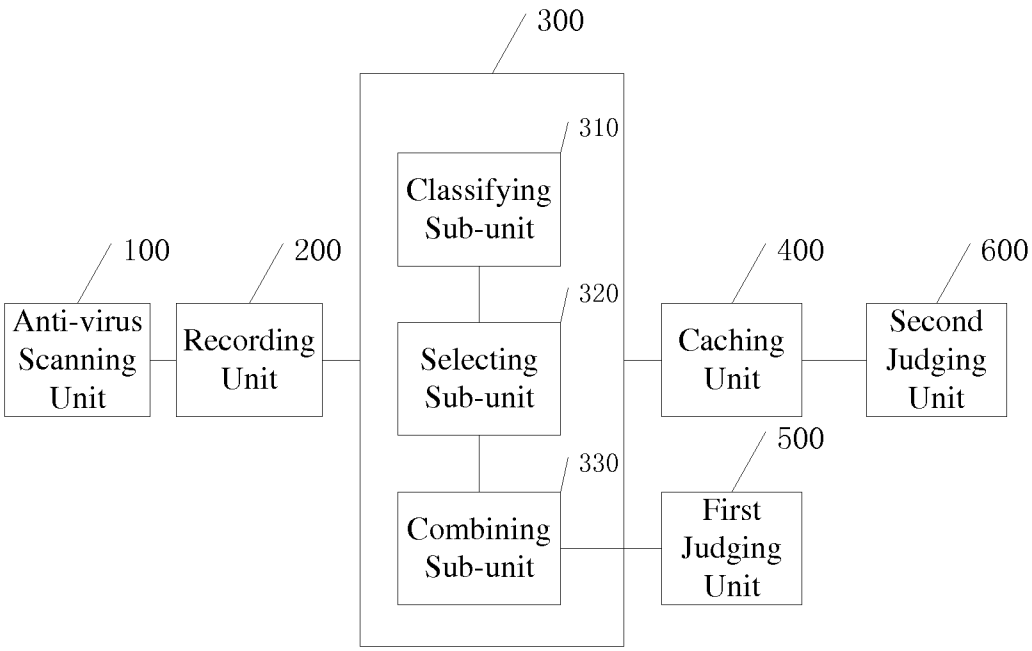
300
310
Classifying Sub-unit
100
200
400
600
320
Anti-virus Scanning Unit
Recording Unit
Selecting Sub-unit
Caching Unit
Second Judging Unit
500
330
Combining Sub-unit
First Judging Unit

Fig. 8

# INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2013/087166

**A. CLASSIFICATION OF SUBJECT MATTER**

G06F 21/00 (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: G06F 21/-

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

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

CNABS;CPRSABS; CNTXT; DWPI;

anti-virus, scan, file, disk, record+, analys+, threshold, load, cache, reference, memory, kill+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| Y | CN102737187 A(TENCENT TECHNOLOGY SHENZHEN CO LTD) 17 Oct.2012(17.10.2012) see the abstract | 1-2,6-7 |
| A | | 3-5,8-10 |
| Y | CN1409222 A(RUIXING SCI & TECHNOLOGY CO LTD BEIJING) 09 Apr. 2003(09.04.2003) see the abstract | 1-2,6-7 |
| A | | 3-5,8-10 |
| A | US7591019 B1(KASPERSKY LAB ZAO) 15 Sep. 2009(15.09.2009) see the whole document | 1-10 |

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

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"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)

"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

"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

"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

"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

"&"document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 05 Feb. 2014(05.02.2014) | **27 Feb. 2014 (27.02.2014)** |
| Name and mailing address of the ISA/CN<br>The State Intellectual Property Office, the P.R.China<br>6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China 100088<br>Facsimile No. 86-10-62019451 | Authorized officer<br>LI, Xiaoqing<br>Telephone No. (86-10)6241 1822 |

Form PCT/ISA /210 (second sheet) (July 2009)

# INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2013/087166

| Patent Documents referred in the Report | Publication Date | Patent Family | Publication Date |
|---|---|---|---|
| CN102737187 A | 17.10.2012 | None | |
| CN1409222 A | 09.04.2003 | CN1282083C | 25.10.2006 |
| US7591019 B1 | 15.09.2009 | EP2237185 A3 | 05.09.2012 |
| | | EP2237185 A2 | 06.10.2010 |
| | | EP2237185B1 | 04.12.2013 |