



(51) International Patent Classification:

G06F 17/30 (2006.01) G06F 17/00 (2006.01)

(21) International Application Number:

PCT/US2015/051376

(22) International Filing Date:

22 September 2015 (22.09.2015)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

1250/CHE/2015 13 March 2015 (13.03.2015) IN

(71) Applicant: HEWLETT PACKARD ENTERPRISE DEVELOPMENT LP [US/US]; 11445 Compaq Center Drive West, Houston, TX 77070 (US).

(72) Inventors: KARUPPUSAMY, Ramesh Kannan; Sy.No.192, Whitefield Road, Mahadevapura Post, Bangalore, Karnataka 560048 (IN). KANNAN, Rajkumar; Sy.No.192, Whitefield Road, Mahadevapura Post, Bangalore, Karnataka 560048 (IN). PATHANIPADATH KARTHIKEYAN, Arun Vishnu; Sy.No.192, Whitefield Road, Mahadevapura Post, Bangalore, Karnataka 560048 (IN).

(74) Agents: ORTEGA, Arthur S. et al.; Hewlett Packard Enterprise, 3404 E. Harmony Road, Mail Stop 79, Fort Collins, CO 80528 (US).

(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, 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, ST, 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).

Declarations under Rule 4.17:

- as to the identity of the inventor (Rule 4.17(i))
- as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))
- as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))

Published:

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

(54) Title: FILE MANAGEMENT

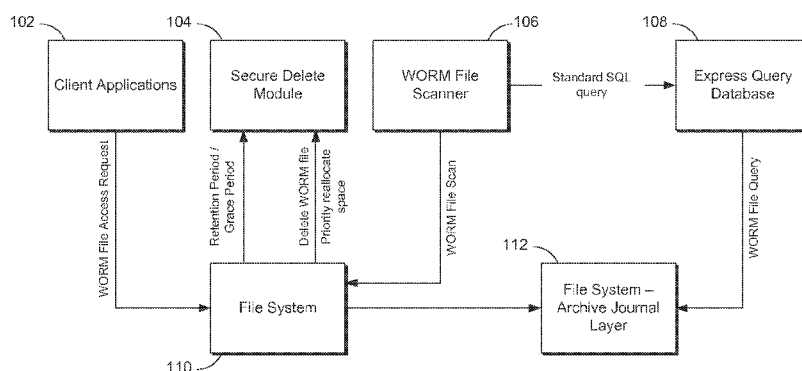


FIG. 1

(57) Abstract: According to an example, to provide for file management on a storage device, a request to access a file on a file system is received. A determination is made if a retention period and a grace period associated with the file have expired. In the event that the retention period and the grace period associated with the file have expired, access to the file is denied, a delete command is sent to a delete module, a data block associated with the file is shredded, and the data block is freed on the computing device. In an example, the data block is set for priority reallocation in the file system



FILE MANAGEMENT

BACKGROUND

[0001] Computing systems, devices, and electronic components in general may be sold or configured with a storage device or disk drive, such as a hard disk drive or a solid state drive. Storage devices may include a file system comprising the logic and structure to store and retrieve data on the storage device, which may be stored in the form of digital files that contain private, confidential, or sensitive data with various levels of security requirements. Files on the storage device may be deleted or otherwise removed from the storage device.

BRIEF DESCRIPTION OF THE DRAWINGS

[0002] FIG. 1 illustrates a system for deleting a file on a storage device and reallocating storage space, according to an example of the present disclosure;

[0003] FIG. 2 illustrates a flowchart of receiving a request to access a file and reallocating storage space, according to an example of the present disclosure;

[0004] FIG. 3 illustrates a flowchart of querying a file system for files and reallocating storage space, according to an example of the present disclosure; and

[0005] FIG. 4 illustrates a schematic representation of a computing device that may be used as a platform for implementing or executing at least one of the processes depicted in FIGS. 2-3, according to an example of the present disclosure.

DETAILED DESCRIPTION

[0006] Various examples described below provide for the secure deletion of files on a storage device or disk drive (referred to collectively herein as a “disk drive” or “disk”). In some examples, the secure deletion of files may include denying access to a file marked as a write-once read-only file after a retention and/or grace period have expired, running a single or multiple pass erasure on the disk block or blocks associated with the file, and reallocating the erased blocks for priority re-allocation or re-use in the file system to be overwritten with new data.

[0007] Generally, computing systems, devices, and electronic components such as desktop computers, laptop computers, servers, thin clients, tablets, smartphones, digital video recorders, retail point of sale devices, and other computing equipment (hereinafter “device” or “devices”) may comprise a storage device or disk drive, such as a hard disk, solid state disk, flash memory or flash disk, or other storage device capable of storing data for use by the device.

[0008] Disk drives may store data that is highly confidential, private, or sensitive, including personal data in the consumer electronics sector; financial or medical data in the commercial sector; and/or product and design data in the industrial sector, as examples. Disk drives may be susceptible to various techniques to recover or restore data that was deleted or marked for erasure by a file system or an operating system. For example, a file may be deleted by an operating system by deleting a pointer to the file in a file allocation table, making the file effectively deleted for purposes of the operating system, but the file itself may remain on a disk drive until overwritten, such as when additional space is needed on the disk drive for a new, copied, or moved file.

[0009] Various techniques may be employed to attempt to “shred” or “wipe” or securely erase a file that a user wishes to delete to minimize data remanence, i.e., a residual representation of digital data that remains on a disk after normal file deletion. For example, disk blocks, sectors, bytes, or bits (collectively referred to herein as “blocks” or “data blocks”) on a disk drive associated with a file may be overwritten with, for examples, zeroes or random data.

[0010] In some examples, a file to be shredded may be overwritten many times, such as thirty-five times or “passes” to reduce the ability of various data recovery techniques to successfully recover the file. File shredding may, however, reduce disk performance and generally require increased system resources, especially as the number of passes increases.

[0011] Files that are deleted or securely erased may be later overwritten in the normal course of using a file system, such as when a new file is created, or when a file is copied or moved, by reusing disk blocks associated with the file that was previously deleted or securely erased as a place to store new data. When the disk blocks are overwritten in the normal course of file system usage, the ability to recover the deleted or securely erased file is further decreased even if the file or disk blocks being overwritten were simply deleted in a file allocation table, or only wiped with a low number of passes.

[0012] In some examples, however, there may be a gap between the time a file is deleted or securely erased and the time the file is later overwritten by the file system. In such examples, the disk blocks associated with the file may be left lingering unused or unallocated for long periods of time. Such gaps may be

especially long in the case of write-once read-many ("WORM") files that may have been retained on a disk following a long retention period.

[0013] According to an example described herein, to provide for file management on a storage device, a request to access a file on a file system is received. A determination is made if a retention period and a grace period associated with the file have expired. In the event that the retention period and the grace period associated with the file have expired, access to the file is denied, a delete command is sent to a delete module, a disk block associated with the file is shredded, and the disk block is freed on the computing device. In an example, the disk block is set for priority reallocation or re-use in the file system.

[0014] FIG. 1 illustrates a system for deleting a file on a disk drive and reallocating disk space, according to an example of the present disclosure. The system 100 of FIG. 1 may be resident on a computing device, such as the desktop computer, laptop computer, server, thin client, tablet, smartphone, digital video recorder, retail point of sale device, or other computing equipment discussed above. In some examples, the system of FIG. 1 may reside on a disk drive on a computing device, while in other examples the system of FIG. 1 may be distributed on different components contained in a computing device, such as on a disk and a separate disk controller.

[0015] System 100 may include a file system 110, which may be stored on or accessible by a disk drive on a computing device. A file system (or file management system) may be used to control how data is stored and/or retrieved on a disk by separating data into pieces or chunks on the disk, e.g., as files, and managing the files

with structure, logic, and other rules. In some examples, the files may be associated with or organized by filenames, directories, metadata and other attributes. In some examples, a file system may be virtual in that files exist as mappings to another data store. The file system may also be responsible for deleting files in the file system and/or securely deleting files through the shredding and/or wiping techniques discussed herein.

[0016] File system 110 may also comprise, in an example, an archive journal layer 112. The files stored on file system 110 may be archival files, i.e., files not used by a user in everyday use, but intended to be archived without deletion, or deleted after given date or period of time.

[0017] A user may access file system 110 through client applications 102, which may include an operating system, software applications such as file managers, archival systems, word processors, e-mail clients, photography tools, music library tools, web browsers, or other software applications capable of creating, retrieving, deleting, archiving, or otherwise processing a file.

[0018] Client applications 102 and file system 110 and/or archive journal layer 112 may be capable of applying a retention period value to a file, and/or a grace or “cool-off” period to a file. For example, a file created by a user on client application 102 may be stored on file system 110 with a retention period of one year and a grace period of one month. In such an example, the file could not be deleted prior to the expiration of a one year period beginning from the time the file was created or the last time the file was accessed or archived, plus a grace period of one month to enable a user to recover a file within a timeframe.

[0019] Retention periods and/or grace periods may be governed by, for example, laws, compliance rules, or security restrictions which may be enforced by policies stored on a file system or other component, or which may be selected by a user. Retention periods and/or grace periods may be stored in databases, within files, or in metadata associated with files, as examples. A grace period may be set to zero in cases where high security is required, or a value greater than zero to protect against accidental deletion, even after a required retention period is satisfied.

[0020] In some examples, once a file that has been archived has satisfied a retention and/or grace period, the file may remain or be stored as a WORM file on the disk drive in perpetuity, with or without the ability to overwrite a disk block associated with the file, or with the ability to overwrite the file using a manual or tedious administrative process or third-party utility, outside of a native file system. Such a process may be considered a “disk cleanup” to restore available space to a file system by removing files that no longer need to be retained.

[0021] System 100 may also include a delete module or secure delete module 104 to delete, shred, wipe, or otherwise securely delete a file or disk space associated with a file at the block, sector, byte, or bit level. Secure delete module 104 may be part of a file system, part of a disk drive firmware (or machine readable instructions), part of a disk drive controller, part of an operating system, or a daemon, as examples. Module 104 may delete a file by removing a pointer to the file in a file allocation table, or may be actually delete or overwrite blocks, sectors, bytes, or bits associated with the file using techniques such as those described herein, including single pass or multiple pass overwrites.

[0022] File system 110 and/or secure delete module 104 may also control or instruct another component or disk module (or disk file management module) to control allocation of disk blocks. Block allocation may include modeling or mapping a physical block address, such as a combination of drive numbers, cylinder numbers, track numbers, and/or sector numbers on a disk, to a block address accessible by the file system. In some examples, block allocation may be controlled by reading or writing to a block allocation map, i.e., a data structure used to track disk blocks that are considered in use.

[0023] In an example, file system 110 may include or communicate with a disk module for disk block allocation and instruct the module to prioritize block allocation to a block that was just deleted, such that when new data is written to the disk, the data is written over the block associated with the just-deleted file to further decrease the ability to recover the deleted data in that block. In another example, such as when multiple files are deleted, file system 110 may include or communicate with a queue to allow for prioritized re-use or reallocation of a disk block based on a position in the queue. In both examples, the amount of time between when a file is deleted and when new data is overwritten in the same disk block space may be minimized.

[0024] System 110 may also include a WORM file scanner 106 to locate files and/or a database 108 to query file system 110 or archive journal layer 112 for files in a WORM state, or files ready for deletion after a retention period and grace period have expired. WORM file scanner 106 and/or database 108 may be considered part of a cleanup process, and may be based on a schedule.

[0025] FIG. 2 illustrates a flowchart of receiving a request to access a file and reallocating disk space, according to an example of the present disclosure.

[0026] In block 202, a request to access a file is received from, e.g., a user or a process. The requested file may be a WORM file or, generally, a file that has been archived. The file request may be received through an operating system, file manager, archival tool, or any other software operating on the computing device or a remote computing device.

[0027] In block 204, a determination is made as to whether the file retention period and grace period have expired, e.g., as in the example above of a file with a one year retention period and a one month grace period. If the periods have expired, i.e., if the current time is at least one year, one month, and one second after the file was created, last accessed, or archived, flow proceeds to block 208.

[0028] In block 208, access to the file is denied, as the file is no longer in a state where retention is required or where a grace period is available, and the file is identified for deletion. In block 208, an "Access Denied" message or a "File Does Not Exist" message may be returned to the requestor or caller. In other examples, a message may explain that the file is no longer being retained and will be deleted from the disk, with options for a user to securely delete the file.

[0029] In block 210, a delete command is sent to a delete module or other file system or disk component responsible for deleting a file, as discussed above. In block 212, the blocks associated with the file are shredded. As discussed above, shredding a file or disk block(s), sector(s), byte(s), or bit(s) associated with the file

may comprise overwriting the freed areas with random numbers, characters, or zeroes for a number of times or passes based on a desired security level.

[0030] In block 214, the blocks freed in block 212 are set for priority reallocation or reuse by the disk and/or file system. In some examples, priority reallocation may mean that the freed blocks will be the next blocks to be overwritten by new data stored on the disk by the file system.

[0031] In other examples, the freed blocks may be added to a disk block overwrite queue of freed blocks, with the queue allocating blocks to new data in a first-in, first-out ("FIFO") manner. For example, if five files are deleted, the blocks associated with the five files may be added to the queue in the order they are deleted, and those blocks may be overwritten with new data in that order.

[0032] In some examples, the queue may be further prioritized based on other attributes of a freed block, such as the security or sensitivity level of the file that was previously stored on that block, or the number of times the data was overwritten, with prioritization enabled by the file system or a prioritization module associated with the file system. For example, a file overwritten one time may have the highest level of priority reallocation as compared to a file that was overwritten seven times.

[0033] In examples where the retention period and/or grace period have not expired, flow may proceed to block 206, where access to the file is granted or permitted. A user may be presented with a message indicating the date and/or time the file is to be deleted following a retention period and/or grace period, with options to extend the retention and/or grace periods.

[0034] FIG. 3 illustrates a flowchart of querying a file system for files and reallocating disk space, according to an example of the present disclosure. In FIG. 3, as opposed to receiving a request from a user or process for access to a file, the file system may be queried by a process, routine, script, or database tool. The query may be run on a periodic or scheduled basis, such as a schedule to “free up” or “clean up” a disk, or increase the security level of deleted space on the disk. The flow of FIG. 3 may be particularly useful to securely clean up disk space associated with blocks that are past a retention period and grace period but that have not been accessed by a user or process, such as to trigger the flow of FIG. 2.

[0035] In block 302, the file system is queried for files stored on the disk drive with an expired retention period. In block 304, a determination is made as to whether the grace period associated with the file has expired. If the grace period has not expired, access to the file may be permitted or the query may simply continue running in block 306, i.e., looping through files on the file system or metadata for each file.

[0036] If the grace period has expired, flow may proceed to block 308 where requests to access the file, if any, are denied, or where metadata or a table is updated to reflect that the file is no longer accessible. Flow may then proceed to block 310, where the file is deleted. In block 312, the blocks associated with the file may be shredded as described above.

[0037] In block 314, according to an example, the blocks on the disk drive and/or on the file system for the shredded file may be set as the first available blocks for the next block allocation request received from the disk drive, i.e., a request to

locate available or unused disk blocks to store new data. As discussed above, block 314 may comprise updating a queue to prioritize block allocation such that blocks associated with files shredded in block 312 are overwritten prior to other areas of the disk, and in an order specified by the queue.

[0038] The flow of FIG. 3 may also allow for the ability to output a report, statistics, analytics, or other data indicating the total space reclaimed by the flow of FIG. 3, thereby illustrating the administrative and storage benefits on a dollar, performance, and/or file size basis.

[0039] FIG. 4 illustrates a schematic representation of a computing device that may be used as a platform for implementing or executing at least one of the processes depicted in FIGS. 2-3, according to an example of the present disclosure

[0040] In an example, device 400 comprises a processing resource, processor, or CPU 402; a memory 404; a disk drive or storage 406; a power source 408; a disk controller 410; and/or a firmware (or machine readable instructions) 412. Storage 406 may be a hard disk drive, a solid state drive, a flash memory, or other storage, and may include a file system such as described above. Disk controller 410 may enable communication between storage 406 and processing resource 402. The CPU 402, memory 404, disk drive or storage 406, and disk controller 410 may be coupled by a bus or other interconnect.

[0041] In some examples, device 400 may also comprise a computer readable medium that may comprise an operating system, applications, and disk tools. Disk tools may include, for example, modules to delete files, or securely delete or wipe

files by, for example, overwriting the file or disk blocks associated with the file with random numbers, characters, or zeroes.

[0042] Some or all of the operations set forth in the figures may be contained as a utility, program, or subprogram in any desired computer readable storage medium, or embedded on hardware. In addition, the operations may be embodied by machine-readable instructions. For example, they may exist as machine-readable instructions in source code, object code, executable code, or other formats. The computer readable medium may also store other machine-readable instructions, including instructions downloaded from a network or the internet.

[0043] The computer-readable medium may store instructions to scan a file system for a write-once read-many file with a satisfied retention period, deny access to a file with an expired retention period and an expired grace period, execute a single-pass (or multi-pass) erasure of the file system space associated with the file, and add an overwrite instruction to a priority allocation queue for the file system space associated with the file.

[0044] The computer-readable medium may also store a firmware that may perform basic tasks such as recognizing input from input devices, such as a keyboard or a keypad; sending output to a display; keeping track of files and directories on a computer readable medium; controlling peripheral devices, such as drives, printers, or image capture devices; and managing traffic on a bus. The network applications may include various components for establishing and maintaining network connections, such as machine readable instructions for implementing

communication protocols including but not limited to TCP/IP, HTTP, HTTPS, Ethernet, USB, and FireWire.

[0045] The above discussion is meant to be illustrative of the principles and various embodiments of the present disclosure. Numerous variations and modifications will become apparent once the above disclosure is fully appreciated. It is intended that the following claims be interpreted to embrace all such variations and modifications.

CLAIMS

What is claimed is:

1. A method of file management on a storage device, comprising:

receiving, on a computing device, a request to access a file on a file system;

determining if a retention period and a grace period associated with the file have expired; and

in the event that the retention period and the grace period associated with the file have expired, denying access to the file, sending a delete command to a delete module, shredding a data block associated with the file, and freeing the data block on the computing device,

wherein freeing the data block further comprises setting the data block for priority reallocation in the file system.
2. The method according to claim 1, wherein the file is a write-once read-many file.
3. The method according to claim 1, wherein setting the data block for priority reallocation in the file system comprises setting the data block to be the next data block to be overwritten on the computing device.

4. The method according to claim 1, wherein setting the data block for priority reallocation in the file system comprises adding the data block to a data block overwrite queue on a storage device.
5. The method according to claim 1, wherein shredding the data block associated with the file comprises executing a single-pass erasure.
6. The method according to claim 1, wherein shredding the data block associated with the file comprises executing a multiple-pass erasure.
7. The method according to claim 1, wherein the retention period and the grace period are user-selectable.
8. A computing device comprising:
 - a processor to manage the computing device; and
 - a disk file management module to query a file system for a file with a retention period and a grace period value, deny access to a file with an expired retention period and an expired grace period, execute a delete instruction on the file, shred a file system block associated with the file, and set the file system block as available for the next block allocation request from the file system.
9. The computing device according to claim 8, wherein the computing device further comprises a module to prioritize disk block allocation in a queue.

10. The computing device according to claim 9, wherein the queue is prioritized based on sensitivity levels of deleted files.

11. The computing device according to claim 8, wherein the disk file management module is to automatically query the file system on a scheduled basis.

12. The computing device according to claim 8, wherein the file system is a virtual file system.

13. The computing device according to claim 8, wherein the file system is an indexed journal.

14. A non-transitory computer readable storage medium on which is stored a computer program, said computer program to provide for file management, said computer program comprising instructions to:

scan a file system for a write-once read-many file with a satisfied retention period;

deny access to a file with an expired retention period and an expired grace period;

execute at least a single-pass erasure of the file system space associated with the file; and

add an overwrite instruction to a priority block allocation queue for the file system space associated with the file.

15. The computer readable storage medium according to claim 14, wherein the order of the priority block allocation queue is based on a number of erasure passes of the file system space associated with the file.

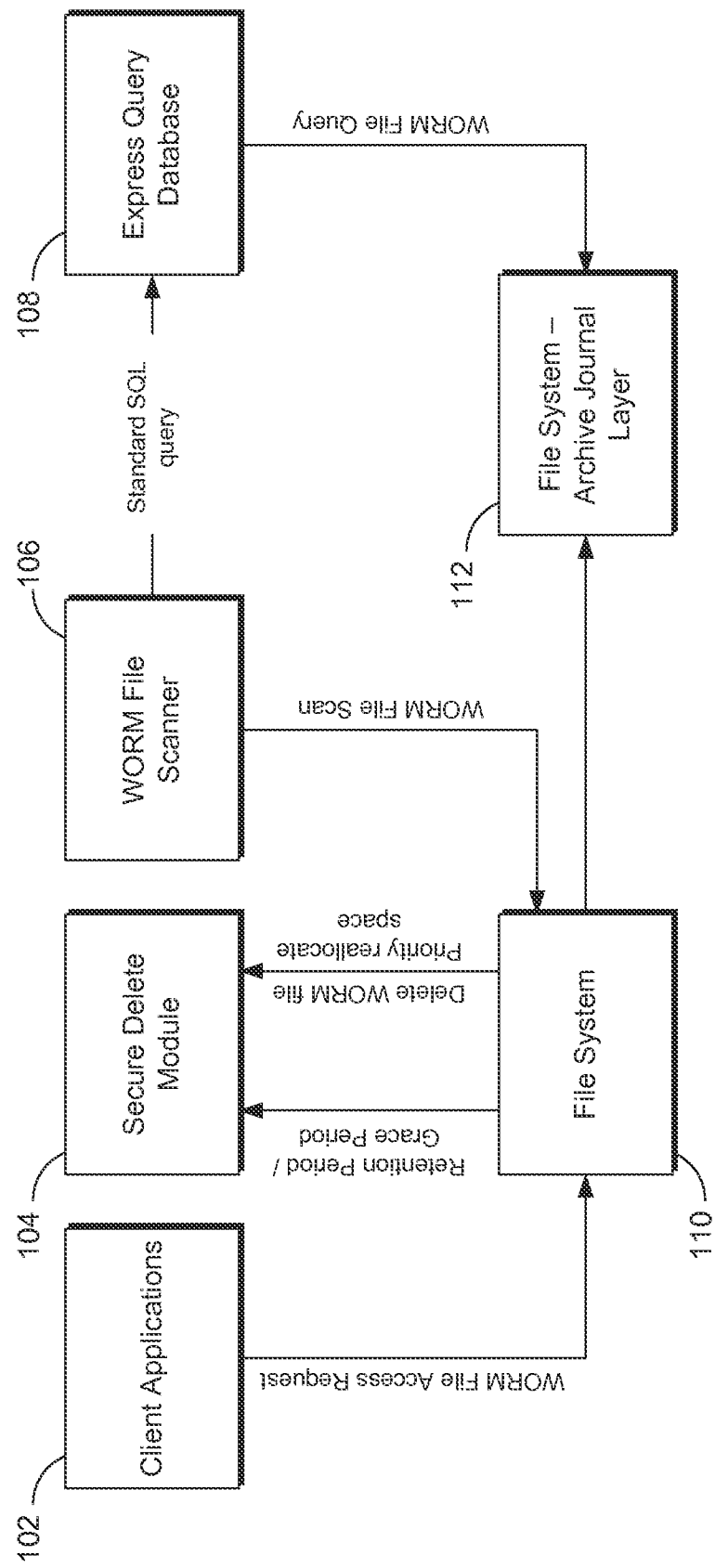


FIG. 1

2/4

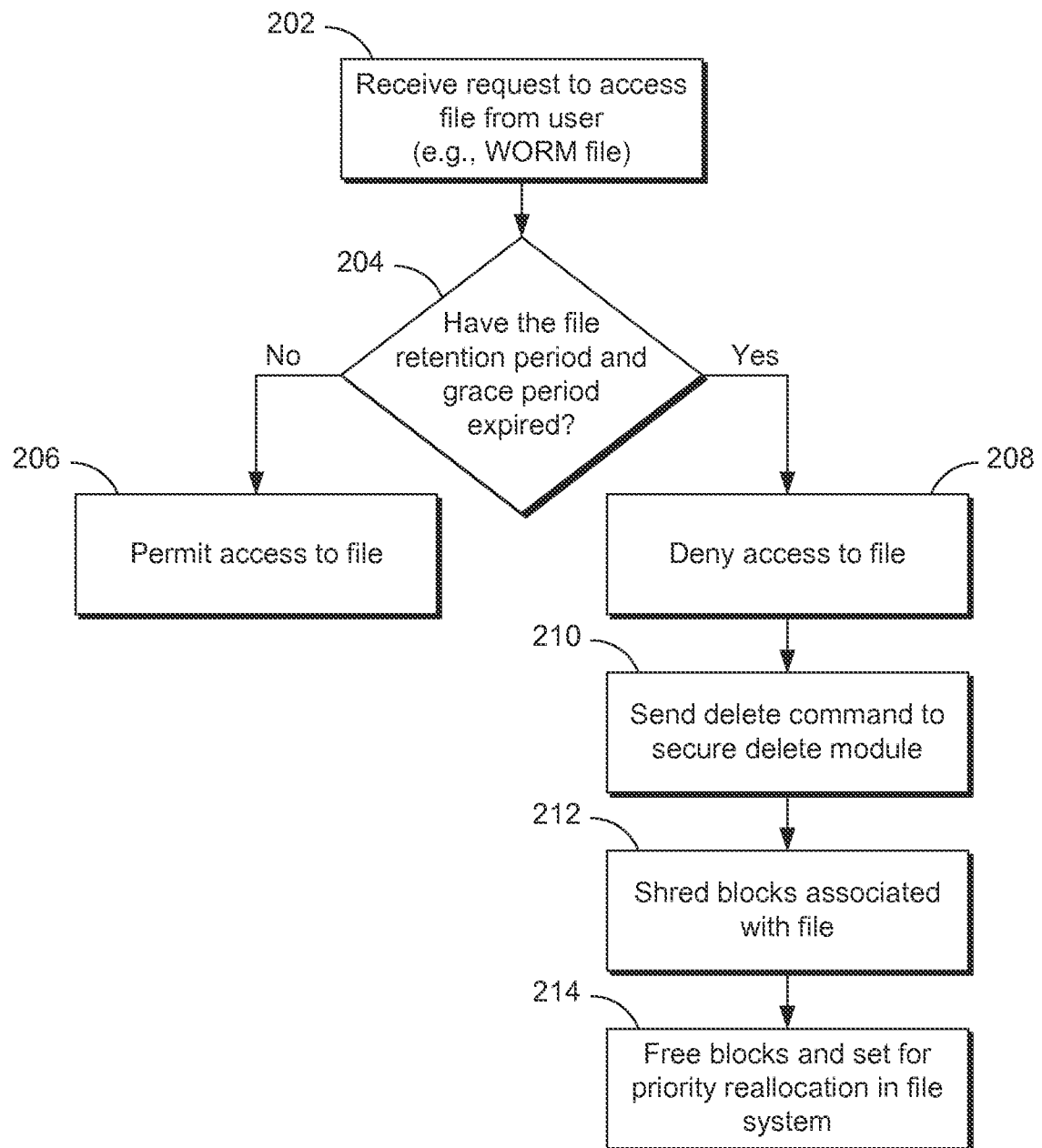


FIG. 2

3/4

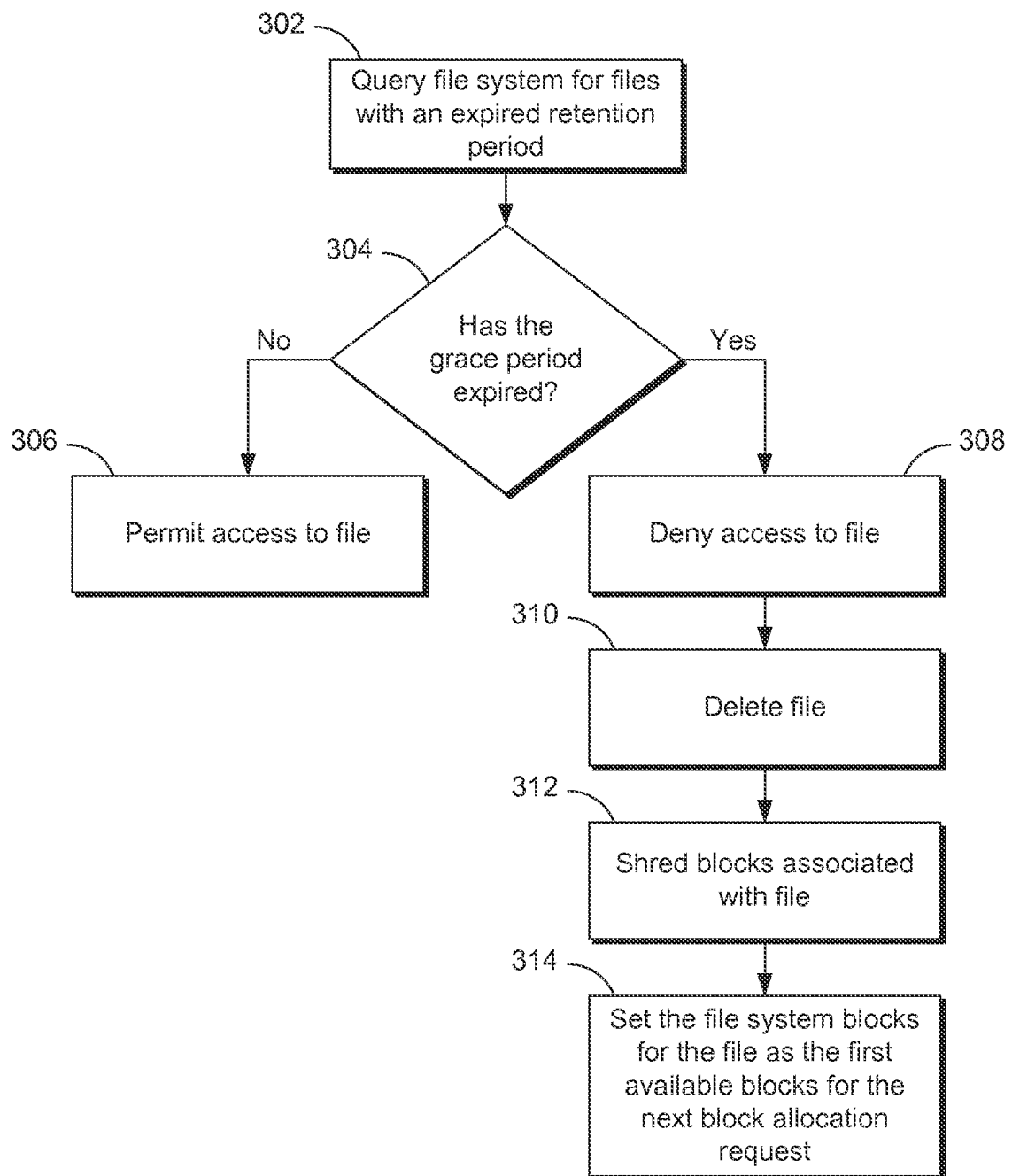


FIG. 3

4/4

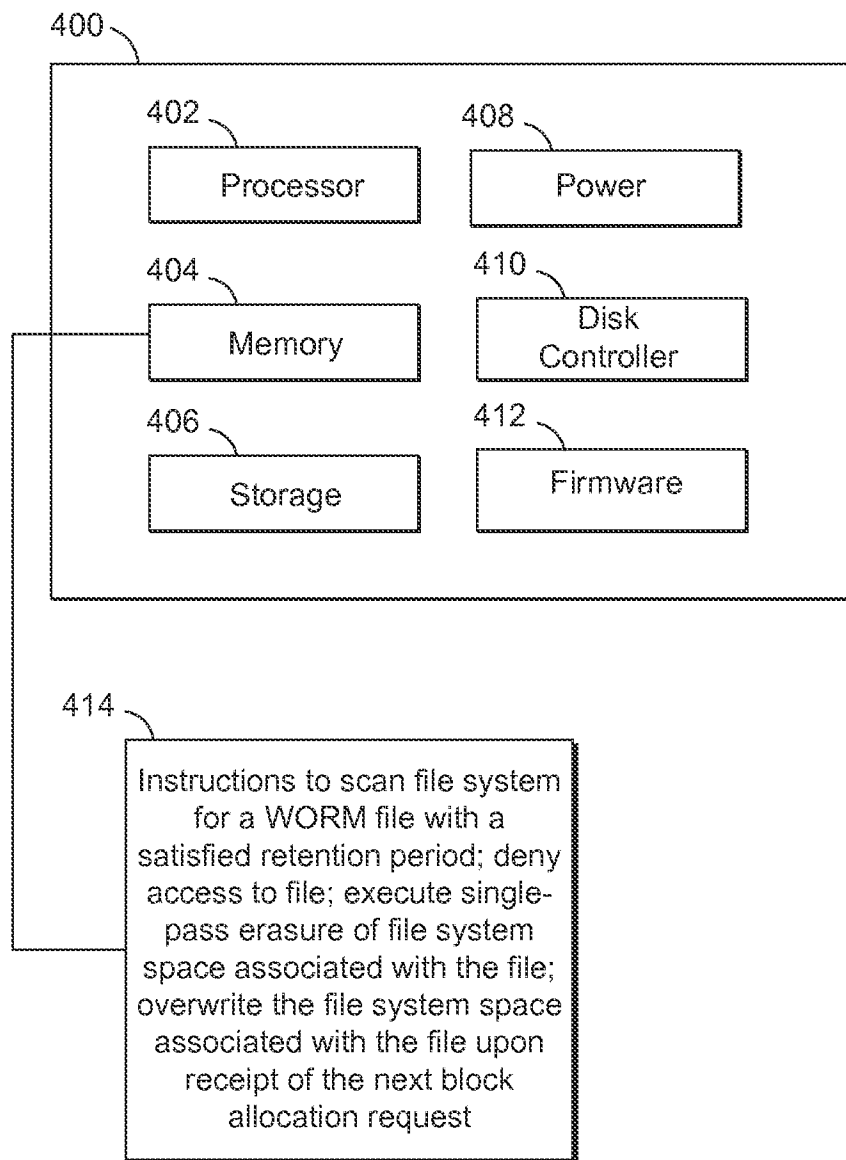


FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2015/051376**A. CLASSIFICATION OF SUBJECT MATTER****G06F 17/30(2006.01)i, G06F 17/00(2006.01)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)

G06F 17/30; G06F 7/00; G06F 11/00; G06F 17/00

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

Korean utility models and applications for utility models

Japanese utility models and applications for utility models

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

eKOMPASS(KIPO internal) & Keywords: file, deletion, retention period, grace period, expired, shred, priority, and similar terms.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2014- 0330800 A1 (KCM NETWORKS INC.) 06 November 2014 See paragraphs [0043]-[0044], [0050]-[0051], [0068], and [0111]-[0112]; claim 27; and figures 3A-3B and 6.	1- 15
Y	US 2008- 0104150 A1 (WILLIAM H. MOORE et al.) 01 May 2008 See paragraphs [0045]-[0049] and [0066]; claim 1; and figure 7D.	1- 15
A	US 2005- 0125411 A1 (MICHAEL KILIAN et al.) 09 June 2005 See paragraphs [0048]-[0050] and figure 4.	1- 15
A	US 2010- 0332563 A1 (YOSHI AKI FUJIKAWA) 30 December 2010 See paragraphs [0212]-[0215] and figure 14.	1- 15
A	US 2007- 0050686 A1 (KIMBERLY KEETON et al.) 01 March 2007 See paragraphs [0080]-[0083] and figures 6-7.	1- 15



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

16 December 2015 (16.12.2015)

Date of mailing of the international search report

16 December 2015 (16.12.2015)

Name and mailing address of the ISA/KR

International Application Division

Korean Intellectual Property Office

189 Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea



Facsimile No. +82-42-472-7140

Authorized officer

NHO, Ji Myong

Telephone No. +82-42-481-8528



INTERNATIONAL SEARCH REPORT

International application No.

PCT/US2015/051376

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.

INTERNATIONAL SEARCH REPORTInternational application No.
PCT/US2015/051376**Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)**

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:
2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fees, this Authority did not invite payment of any additional fees.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

- ☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.
- ☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.
- ☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2015/051376

Box No. IV Text of the abstract (Continuation of item 5 of the first sheet)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2015/051376

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2014- 0330800 A1	06/11/2014	AU 9016701 A CA 2393787 A1 CA 2393787 C CA 2788750 A1 US 2006- 010150 A1 US 2008- 263112 A1 US 7392234 B2 US 8782009 B2 WO 02- 25445 A2 WO 02- 25445 A3 WO 02- 25445 A9	02/04/2002 28/03/2002 28/08/2012 28/03/2002 12/01/2006 23/10/2008 24/06/2008 15/07/2014 28/03/2002 31/12/2003 08/05/2003
US 2008- 0104150 A1	01/05/2008	US 7584229 B2	01/09/2009
US 2005- 0125411 A1	09/06/2005	CN 1629826 A DE 102004056651 A1 GB 2409547 A J P 2005- 174339 A US 9075851 B2	22/06/2005 07/07/2005 29/06/2005 30/06/2005 07/07/2015
US 2010- 0332563 A1	30/12/2010	J P 2011- 008621 A	13/01/2011
US 2007- 0050686 A1	01/03/2007	US 7467333 B2	16/12/2008

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2015/051376

Continued on Next Page

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2015/051376

Continued on Next Page