



(51) International Patent Classification:  
*G06F 11/08* (2006.01)

(21) International Application Number:  
PCT/US2011/034563

(22) International Filing Date:  
29 April 2011 (29.04.2011)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:  
12/775,205 6 May 2010 (06.05.2010) US

(71) Applicant (for all designated States except US): **UTC FIRE & SECURITY AMERICAS CORPORATION, INC.** [US/US]; 8985 Town Center Parkway, Bradenton, Florida 67525 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **POTTER, Timothy Stevens** [US/US]; 6215 217th Street E, Bradenton, Florida 34211 (US). **BECKER, Donald** [US/US]; 12002 Clubhouse Drive, Bradenton, Florida 34202 (US). **MONTGOMERY, Bruce Ray, Jr.** [US/US]; 530 Silk Oak Drive, Venice, Florida 34293 (US). **DOPSON, Dave** [US/US]; 2033 2nd Avenue, Seattle, Washington 98101 (US).

(74) Agents: **KOENCK, Alan, M.** et al.; Kinney & Lange, P.A., The Kinney & Lange Building, 312 South Third Street, Minneapolis, MN 55415 (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, 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, IS, JP, KE, KG, KM, 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, PE, PG, PH, PL, PT, RO, RS, RU, 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.

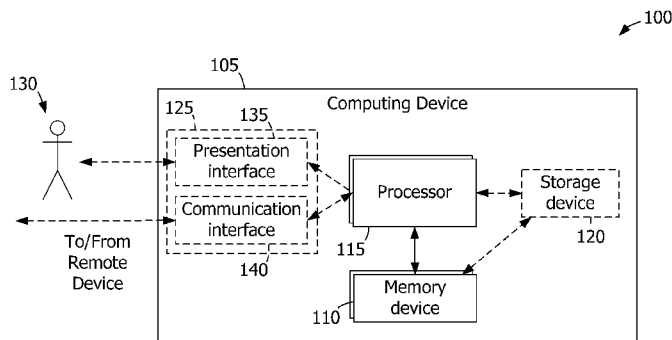
(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, 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, ML, MR, NE, SN, TD, TG).

Published:

— without international search report and to be republished upon receipt of that report (Rule 48.2(g))

(54) Title: METHODS AND SYSTEM FOR VERIFYING MEMORY DEVICE INTEGRITY

FIG. 1



(57) Abstract: A method and system for verifying memory device integrity includes identifying at least one memory block corresponding to at least one memory location within a memory device. The memory block is associated with a portion of a file and a checksum representing data within the memory block at a first time. Based at least in part on determining that the memory block is mapped to the same portion of the same file at a second time, it is indicated that the checksum represents expected data within the memory block. A system for verifying memory device integrity is also disclosed.

WO 2012/015503 A2

## METHODS AND SYSTEM FOR VERIFYING MEMORY DEVICE INTEGRITY

### BACKGROUND OF THE INVENTION

#### Field of the Invention

5           The embodiments described herein relate generally to verifying memory device integrity and, more particularly, to memory verification in an online computing device.

#### Description of Related Art

10           It is known to use checksum-based systems to verify the integrity of computer memory in limited scenarios. For example, error-correcting code (ECC) random access memory (RAM) detects memory errors but performs such error detection only as specific portions of the memory are accessed. It is also known to verify memory integrity in an offline mode, such as by executing a memory test utility in place of a conventional operating system.

15           However, existing systems and methods do not provide for continuous memory verification while a computer is online, executing one or more application programs within a demand paged operating system. Especially in computing devices where high reliability over an extended period is required, verification of proper memory device function is essential. For example, some high-reliability systems operate for months or years with little activity but are expected to function flawlessly in an emergency.  
20           Accordingly, a need exists for continuous online memory verification in a computing device.

### BRIEF SUMMARY OF THE INVENTION

25           In one aspect, a method for verifying an integrity of a memory device is provided. The method includes identifying, by a processor coupled to the memory device, a memory block corresponding to at least one memory location within the memory device. The memory block is associated with a first portion of a first file to which the memory block is mapped at a first time and a prior checksum representing data within the memory block at the first time. It is determined, by the processor, whether the identified memory block is mapped to the first portion of the first file at a second time  
30           subsequent to the first time. Based at least in part on determining that the identified memory block is mapped to the first portion of the first file at the second time, it is

indicated, by the processor, that the prior checksum represents expected data within the identified memory block at the second time.

In another aspect, a system for verifying an integrity of a memory device is provided. The system includes a memory device comprising a plurality of memory locations and a processor coupled to the memory device. The processor is programmed to identify a memory block corresponding to at least one memory location of the plurality of memory locations within the memory device and to associate the identified memory block with a first portion of a first file to which the identified memory block is mapped at a first time and a checksum representing data within the identified memory block at the first time. The processor is also programmed to determine whether the identified memory block is mapped to the first portion of the first file at a second time subsequent to the first time. The processor is further programmed to, based at least in part on determining that the identified memory block is mapped to the first portion of the first file at the second time, indicate that the checksum represents expected data within the identified memory block.

In yet another aspect, one or more computer-readable storage media are provided. The computer-readable storage media have computer-executable components for verifying an integrity of a memory device using at least one processor coupled to the memory device. The components include a control component, a fingerprinting component, and a result component. When executed by the at least one processor, the control component causes the processor to identify a memory block corresponding to at least one memory location within the memory device. When executed by the at least one processor, the fingerprinting component causes the processor to associate the identified memory block with a first portion of a first file to which the identified memory block is mapped at a first time and a first checksum representing data within the identified memory block at the first time, and to determine whether the identified memory block is mapped to the first portion of the first file at a second time. When executed by the at least one processor, the result component causes the processor to calculate a second checksum representing data within the identified memory block at the second time when the identified memory block is mapped to the first portion of the first file at the second time, and to indicate whether the second checksum is equal to the first checksum.

#### BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

Figs. 1-5 show exemplary embodiments of the systems and methods described

herein.

Fig. 1 is a block diagram of a system with a computing device having a memory device.

Fig. 2 is a flowchart of an exemplary method for verifying an integrity of the  
5 memory device shown in Fig. 1.

Fig. 3 is a block diagram of memory blocks within the memory device shown in Fig. 1.

Fig. 4 is a flowchart of an exemplary method for determining whether a checksum represents expected data within the memory block shown in Fig. 3.

10 Fig. 5 is block diagram of a system including a monitoring computing device coupled in communication with a plurality of monitored computing devices via a network.

#### DETAILED DESCRIPTION OF THE INVENTION

Embodiments of the systems and methods described herein facilitate  
15 continuously verifying memory device integrity within an online computing device. While some embodiments are described in connection with pages of memory mapped to files within a storage device, the embodiments provided herein are operable with any form of memory device. Moreover, the term “file” is used herein to include, without limitation, any collection of non-volatile information, such as an executable application,  
20 an operating system image and/or object, a dynamically linked shared code library, and/or fixed parameter data, whether local or remote to a computing device, suitable for use with the methods described herein.

Furthermore, such embodiments facilitate continuous memory device verification without intercepting write operations to the memory device and without direct  
25 modification to executable instructions of an operating system (OS) kernel. For example, at least some of the operations described herein may be executed by a loadable kernel module that interacts with an operating system kernel and/or by a utility application that executes in “userspace” (i.e., with privileges assigned to a user of the computing device).

30 A technical effect of the systems and methods described herein may include one

or more of the following: (a) identifying a memory block corresponding to at least one memory location within a memory device, the memory block associated with a first portion of a first file to which the memory block is mapped at a first time and a prior checksum representing data within the memory block at the first time; (b) determining  
5 whether the memory block is mapped to the first portion of the first file at a second time subsequent to the first time; and (c) based at least in part on determining that the memory block is mapped to the first portion of the first file at the second time, indicating that the prior checksum represents expected data within the memory block at the second time.

Fig. 1 is a block diagram of a system 100 with a computing device 105.  
10 Computing device 105 includes a memory device 110 and, coupled to memory device 110, a processor 115 for executing instructions. In some embodiments, executable instructions are stored in memory device 110. Computing device 105 is configurable to perform one or more operations described herein by programming processor 115. For example, processor 115 may be programmed by encoding an operation as one or more  
15 executable instructions and providing the executable instructions in memory device 110. Processor 115 may include one or more processing units (e.g., in a multi-core configuration).

Memory device 110 is one or more devices allowing information such as executable instructions and/or other data to be stored and retrieved. Memory device 110  
20 may include one or more computer readable media, such as, but not limited to, dynamic random access memory (DRAM) and/or static random access memory (SRAM).

Computing device 105 may also include a storage device 120. Like memory device 110, storage device 120 allows data to be stored and retrieved. Storage device 120 is coupled to processor 115 and, optionally, to memory device 110. For example,  
25 computing device 105 may provide direct memory access (DMA) between storage device 120 and memory device 110. Storage device 120 may include one or more computer readable media, such as, but not limited to, a solid state disk, a hard disk, battery backed SRAM, and/or a flash memory device. Memory device 110 and/or storage device 120 may be configured to store, without limitation, executable  
30 instructions corresponding to an operating system (OS) (e.g., an OS kernel and/or a kernel module), executable instructions corresponding to an application program, configuration data, program data, a dynamically linked shared code library, and/or any other type of data. Storage device 120 may have a larger memory capacity than a

memory capacity of memory device 110.

In some embodiments, memory device 110 is configured to store a copy of at least a portion of data stored within storage device 120. For example, memory device 110 may be configured to store a copy of executable instructions stored within storage  
5 device 120, and processor 115 may be configured to access and execute the executable instructions from memory device 110.

Computing device 105 also includes at least one notification interface 125 configured to interact with a user 130 and/or a remote device (not shown in Fig. 1). In some embodiments, notification interface 125 includes a presentation interface 135  
10 coupled to processor 115. Presentation interface 135 is configured to present information, such as a verification failure and/or a verification success, to user 130. For example, presentation interface 135 may include a display adapter (not shown in Fig. 1), which is configured to be coupled to a display device, such as a light emitting diode (LED) indicator, a cathode ray tube (CRT), a liquid crystal display (LCD), an organic  
15 LED (OLED) display, and/or an “electronic ink” display. In some embodiments, presentation interface 135 includes one or more display devices.

In addition, or alternatively, presentation interface 135 may include an audio adapter (not shown in Fig. 1), which is configured to be coupled to an audio device, such as a loudspeaker. In some embodiments, presentation interface 135 includes one or more  
20 audio devices.

In some embodiments, notification interface 125 includes a communication interface 140 coupled to processor 115. Communication interface 140 is configured to be coupled in communication with a remote device, such as another computing device 105. For example, communication interface 140 may include, without limitation, a wired  
25 network adapter, a wireless network adapter, and/or a mobile telecommunications .

Fig. 2 is a flowchart of an exemplary method 200 for verifying an integrity of memory device 110. Method 200 is described with reference to Fig. 3, a block diagram of data within memory device 110 and storage device 120. Memory device 110 and storage device 120 each include a plurality of memory locations 150. For example, each  
30 memory location 150 may correspond to one byte of data within memory device 110 and/or storage device 120. Multiple memory locations 150 are organized into memory blocks 155. For example, in memory device 110, a memory block 155 may be referred

to as a “page” of memory. In one embodiment, a page of memory corresponds to 4096 memory locations 150, or four kilobytes (4 kB), although other page sizes are also contemplated.

Method 200 includes identifying 205, by processor 115, at least one memory block 160 of memory blocks 155 corresponding to at least one memory location 150 within memory device 110. For example, memory blocks 155 corresponding to all memory locations 150 within memory device 110 may be identified 205. In another example, identifying 205 memory block 160 includes receiving an address corresponding to a memory location 150 within memory device 110 and identifying memory block 160, which corresponds to (e.g., includes) memory location 150. Memory block 160 may be identified 205 based, at least in part, on a predefined memory block size, such as a page size.

In some embodiments, memory block 160 is a page of virtual memory corresponding to one or more memory locations 150 within memory device 110. The one or more memory locations 150 correspond to one or more memory locations 150 within storage device 120.

In addition, or alternatively, one or more memory blocks 155 corresponding to a single file 165 may be identified 205. As shown in Fig. 3, memory block 160 represents a portion 170 of file 165. The remainder of file 165 is also stored within storage device 120 but is not copied into memory device 110. Identifying 205 memory block 160 may include receiving a file reference that indicates file 165 and identifying memory blocks 155 within memory device 110 that are associated with file 165.

Memory block 160 is associated with a prior checksum, which represents data contained within memory block 160 at a prior time. It is determined 210, by processor 115, whether memory block 160 is designated read-only. For example, processor 115 may be programmed to associate metadata with memory block 160 and to determine 210 whether memory block 160 is read-only based on the metadata. Metadata associated with memory block 160 may include, without limitation, a memory block type (e.g., a compound page), a content type (e.g., a kernel object cache), an access mode (e.g., read-only or read-write), a file mapping attribute (e.g., whether memory block 160 is mapped to a file), and/or a quantity of memory blocks 155 capable of writing data to the mapped file, if any.

A current checksum is calculated 215 by processor 115 based at least in part on data within memory block 160. For example, processor 115 may be programmed to calculate a mathematical summation and/or a hash value of data within memory block 160. It is determined 220, by processor 115, whether the prior checksum represents expected data within memory block 160. For example, metadata associated with memory block 160 may be used to determine 220 whether the prior checksum represents expected data, as described below with regard to Fig. 4.

When memory block 160 is designated read-only, and the prior checksum represents expected data within memory block 160, it is determined 225 by processor 115 whether the current checksum is equal to the prior checksum. When the current checksum is not equal to the prior checksum, a verification failure for memory block 160 is indicated 230 via notification interface 125. For example, a verification failure may be indicated 230 by presenting a visible alarm via presentation interface 135, by presenting an audible alarm via presentation interface 135, and/or by transmitting a verification failure message via communication interface 140.

When the prior checksum is determined 220 to not represent expected data within memory block 160, the current checksum may be associated 222 with memory block 160. Upon a subsequent execution of method 200 for memory block 160, the current checksum is regarded as a prior checksum. In other words, the current checksum may be defined as the prior checksum for memory block 160.

In some embodiments, method 200 tracks successful verification of memory block 160. If the current checksum is determined 225 to be equal to the prior checksum, a verification success is indicated 232. For example, processor 115 may be programmed to record (e.g., within memory device 110) a verification success time at which the current checksum was determined 225 to be equal to the prior checksum. In a subsequent execution of method 200, prior to determining 210 whether memory block 160 is designated read-only, processor 115 may be programmed to determine 207 whether memory block 160 was recently successfully verified.

In some embodiments, the recency of a verification success is determined 207 based on a predefined threshold age. For example, the predefined threshold age may be defined as five minutes, thirty minutes, sixty minutes, or any duration of time suitable for use with the methods described herein. In one embodiment, processor 115 is programmed to determine whether the verification success time is older than the

predefined threshold age. For example, a verification success time may be considered older than the predefined threshold age when a current time minus the verification success time is greater than the predefined threshold age. When the verification success time is older than the predefined threshold age, processor 115 is programmed to perform the step(s) of determining 210 whether memory block 160 is designated read-only, calculating 215 a current checksum, determining 220 whether the prior checksum represents expected data within memory block 160, determining 225 whether the current checksum is equal to the prior checksum, and/or indicating 230 a verification failure. Such embodiments facilitate prioritizing the verification of memory blocks 155 which have not recently been verified.

If multiple memory blocks 155 are identified 205, method 200 may include performing the step(s) of determining 210 whether memory block 160 is designated read-only, calculating 215 a current checksum, determining 220 whether the prior checksum represents expected data within memory block 160, determining 225 whether the current checksum is equal to the prior checksum, and/or indicating 230 a verification failure for each identified memory block 155. Prior to processing each identified memory block 155, method 200 may include delaying or “sleeping” for a short duration (e.g., from approximately one millisecond to approximately one second). Such an embodiment facilitates allowing processor 115 to perform operations other than those included in method 200.

Some embodiments facilitate continuous verification of one or more memory blocks 155 of memory device 110. For example, method 200 may be repeated continuously, periodically, or according to any suitable timing. Prior to identifying 205 memory blocks 155, method 200 may include delaying or sleeping for a short period, as described above.

Some embodiments facilitate preventing false verification failures arising from concurrent access to memory block 160. In one embodiment, prior to determining 210 whether memory block 160 is designated read-only, interrupt signals are disabled 209 within processor 115. After determining 225 whether the current checksum is equal to the prior checksum, interrupt signals are enabled 234 in processor 115. In an alternative embodiment, method 200 includes registering 209 for notification of interrupt signals within processor 115. When a notification of an interrupt signal is received after determining 210 whether memory block 160 is designated read-only, processing of

memory block 160 is aborted. For example, processor 115 may be programmed to abort calculating 215 a current checksum, determining 220 whether the prior checksum represents expected data within memory block 160, and/or determining 225 whether the current checksum is equal to the prior checksum.

5 Fig. 4 is a flowchart of an exemplary method 300 for determining 220 whether a checksum represents expected data within memory block 160. In an exemplary embodiment, memory block 160 is associated with a “fingerprint” 175 of metadata associated with memory block 160. Fingerprint 175 includes, without limitation: a file reference 180 indicating file 165, to which memory block 160 is mapped; a page index  
10 185 indicating file portion 170 to which memory block 160 is mapped; a file write count 190 indicating a quantity of write operations executed against file 165; and/or a checksum 195 representing data within memory block 160. Fingerprint 175 may be stored within memory device 110. Moreover, additional metadata may be accessible via file reference 180 and/or page index 185. For example, processor 115 may be  
15 programmed to determine a file status (e.g., “clean” or “dirty”, indicating an absence or presence of pending write operations, respectively) by accessing metadata associated with file reference 180.

In an exemplary embodiment, fingerprint 175 includes one or more static metadata values generated at a first time. At a second time subsequent to the first time,  
20 the static metadata values of fingerprint 175 are considered prior values. Method 300 includes determining 305, by processor 115, whether memory block 160 is mapped to prior file portion 170 indicated by prior file reference 180 and prior page index 185. Based at least in part on determining 305 that memory block 160 is mapped to prior file  
25 portion 170, it is indicated 310, by processor 115, that prior checksum 195 represents expected data within memory block 160. Alternatively, based at least in part on determining 305 that memory block 160 is not mapped to prior file portion 170, it may be indicated 312 that prior checksum 195 does not represent expected data within memory block 160.

Processor 115 may also be programmed to determine 307 whether any write  
30 operations corresponding to file 165 have been executed. For example, processor 115 may be programmed to compare prior file write count 190 from fingerprint 175 to a current write count for file 165. If the current write count is greater than prior file write count 190, it may be determined 307 that one or more write operations have been

executed against file 165 since fingerprint 175 was generated and/or updated (i.e., between the first time and the second time). Processor 115 may be programmed to indicate 310 that prior checksum 195 represents expected data within memory block 160 based further on determining 307 that no such write operations have been executed  
5 between the first time and the second time.

In addition, or alternatively, processor 115 may be programmed to determine 309 whether any write operations corresponding to file 165 are pending at the second time. For example, processor 115 may be programmed to determine 309 whether such write operations are pending based on a file state (e.g., clean or dirty) associated with file  
10 reference 180. Processor 115 may be programmed to indicate 310 that prior checksum 195 represents expected data within memory block 160 based further on determining 309 that no write operations corresponding to file 165 are pending at the second time.

Some embodiments facilitate simplified and/or optimized logic for kernel-related pages. In one embodiment, determining 305 whether memory block 160 is mapped to  
15 prior file portion 170 includes determining 302 whether memory block 160 is allocated to operating system kernel (OS) text. OS kernel text includes, without limitation, executable kernel instructions and/or immutable kernel-related data structures. When memory block 160 is allocated to operating system kernel text, other steps 307, 309 are omitted, and processor 115 is programmed to indicate 310 that prior checksum 195  
20 represents expected data within memory block 160. When memory block 160 is not allocated to operating system kernel text, method 300 proceeds as described above. In another embodiment, determining 210 (shown in Fig. 2) whether memory block 160 is read-only includes determining 302 whether memory block 160 is allocated to operating system kernel text, and allocation of memory block 160 to operating system kernel text  
25 indicates memory-block 160 is read-only.

Some embodiments facilitate associating memory block 160 with current metadata values. For example, when memory block 160 is determined 305 to not be mapped to prior file portion 170, method 300 may include associating 306 memory block  
30 160 with another portion of file 165 or a portion of another file to which memory block 160 is mapped at the second time. In one embodiment, processor 115 is programmed to update file reference 180, page index 185, and/or file write count 190 based on a portion of a file to which memory block 160 is associated at the second time.

Fig. 5 is a block diagram of a system 400 including a monitoring computing

device 405 coupled in communication with a plurality of monitored computing devices 410 via a network 415. For example, monitoring computing device 405 and monitored computing devices 410 may be coupled to network 415 via communication interfaces 140 (shown in Fig. 1). Network 415 may include, without limitation, the Internet, a local area network (LAN), a wide area network (WAN), a wireless LAN (WLAN), a mesh network, and/or a virtual private network (VPN) .

In the exemplary embodiment, monitored computing devices 410 are configured to transmit verification failure messages and/or verification success messages to monitoring computing device 405. Monitoring computing device 405 is configured to receive verification failure messages and/or verification success messages and to indicate corresponding verification failures and/or verification successes, respectively, to user 130 via presentation interface 135 (shown in Fig. 1). Such an embodiment facilitates remote monitoring of a plurality of computing devices 105.

Exemplary embodiments of methods, systems, and computer-readable storage media for use in implementing a memory verification system are described above in detail. The methods, systems, and storage media are not limited to the specific embodiments described herein but, rather, operations of the methods and/or components of the system may be utilized independently and separately from other operations and/or components described herein. Further, the described operations and/or components may also be defined in, or used in combination with, other systems, methods, and/or storage media, and are not limited to practice with only the methods, systems, and storage media as described herein.

A computing device, such as those described herein, includes at least one processor or processing unit and a system memory. The computing device typically has at least some form of computer readable media. By way of example and not limitation, computer readable media include computer storage media and communication media. Computer storage media include volatile and nonvolatile, removable and non-removable physical media implemented in any method or technology for storage of information such as computer readable instructions, data structures, program modules, or other data. Communication media typically embody computer readable instructions, data structures, program modules, or other data in a modulated data signal such as a carrier wave or other transport mechanism and include any information delivery media. Those skilled in the art are familiar with the modulated data signal, which has one or more of its characteristics

set or changed in such a manner as to encode information in the signal. Combinations of any of the above are also included within the scope of computer readable media.

The methods described herein may be encoded as executable instructions embodied in a computer readable medium, including, without limitation, a computer storage medium, a storage device, and/or a memory device. Such instructions, when  
5 executed by a processor, cause the processor to perform at least a portion of the methods described herein.

Although the present invention is described in connection with an exemplary memory verification system environment, embodiments of the invention are operational  
10 with numerous other general purpose or special purpose memory verification system environments or configurations. The memory verification system environment is not intended to suggest any limitation as to the scope of use or functionality of any aspect of the invention. Moreover, the memory verification system environment should not be interpreted as having any dependency or requirement relating to any one or combination  
15 of components illustrated in the exemplary operating environment. Examples of well known memory verification systems, environments, and/or configurations that may be suitable for use with the embodiments described herein include, but are not limited to, embedded computing devices, personal computers, server computers, hand-held or laptop devices, multiprocessor systems, microprocessor-based systems, set top boxes,  
20 programmable consumer electronics, mobile telephones, network PCs, minicomputers, mainframe computers, distributed computing environments that include any of the above systems or devices, and the like.

Embodiments may be described in the general context of computer-executable instructions, such as program components or modules, executed by one or more  
25 computers or other devices. Aspects of the invention may be implemented with any number and organization of components or modules. For example, embodiments are not limited to the specific computer-executable instructions or the specific components or modules illustrated in the figures and described herein. Alternative embodiments may include different computer-executable instructions or components having more or less  
30 functionality than illustrated and described herein.

The order of execution or performance of the operations in the embodiments illustrated and described herein is not essential, unless otherwise specified. That is, the operations may be performed in any order, unless otherwise specified, and embodiments

may include additional or fewer operations than those disclosed herein. For example, it is contemplated that executing or performing a particular operation before, contemporaneously with, or after another operation is within the scope of the described embodiments.

5           Although specific features of various embodiments of the invention may be shown in some drawings and not in others, this is for convenience only. In accordance with the principles of the invention, any feature of a drawing may be referenced and/or claimed in combination with any feature of any other drawing.

10           This written description uses examples to disclose the invention, including the best mode, and also to enable any person skilled in the art to practice the invention, including making and using any devices or systems and performing any incorporated methods. The patentable scope of the invention is defined by the claims, and may include other examples that occur to those skilled in the art. Such other examples are intended to be within the scope of the claims if they have structural elements that do not  
15 differ from the literal language of the claims, or if they include equivalent structural elements with insubstantial differences from the literal language of the claims.

## CLAIMS

## What Is Claimed Is:

1. A method for verifying an integrity of a memory device, the method comprising:  
  
identifying, by a processor coupled to the memory device, a memory block corresponding to at least one memory location within the memory device, the memory block associated with a first portion of a first file to which the memory block is mapped at a first time and a prior checksum representing data within the memory block at the first time;  
  
determining, by the processor, whether the memory block is mapped to the first portion of the first file at a second time subsequent to the first time; and  
  
based at least in part on determining that the memory block is mapped to the first portion of the first file at the second time, indicating, by the processor, that the prior checksum represents expected data within the memory block at the second time.
2. A method in accordance with Claim 1, further comprising indicating that the prior checksum represents expected data within the memory block at the second time based in part on determining that no write operations corresponding to the first file have been executed between the first time and the second time.
3. A method in accordance with Claim 2, further comprising determining that no write operations corresponding to the first file have been executed between the first time and the second time by comparing a first write count associated with the first file at the first time with a second write count associated with the first file at the second time.
4. A method in accordance with Claim 1, further comprising indicating that the prior checksum represents expected data within the memory block at the second time based in part on determining that no write operations corresponding to the first file are pending at the second time.
5. A method in accordance with Claim 1, wherein determining whether the memory block is mapped to the first portion of the first file at the second time comprises determining whether the memory block is allocated to operating system kernel text.

6. A method in accordance with Claim 1, wherein identifying a memory block comprises:

receiving an address corresponding to a first memory location within the memory device; and

identifying a memory block corresponding to the first memory location.

7. A method in accordance with Claim 6, further comprising identifying the memory block based in part on a predefined memory block size.

8. A method in accordance with Claim 1, wherein identifying a memory block comprises identifying a page of virtual memory corresponding to a first memory location within the memory device, the first memory location corresponding to a second memory location within a storage device.

9. A method in accordance with Claim 1, further comprising associating the memory block with a second portion of a second file to which the memory block is mapped at the second time based on determining that the memory block is not mapped to the first portion of the first file at the second time.

10. A method in accordance with Claim 1, further comprising associating, by the processor, the memory block with a second portion of a second file to which the memory block is mapped at the second time based on determining that the memory block is not mapped to the first portion of the first file at the second time.

11. A system for verifying an integrity of a memory device, the system comprising:

a memory device comprising a plurality of memory locations; and

a processor coupled to the memory device and programmed to:

identify a memory block corresponding to at least one memory location of the plurality of memory locations within the memory device;

associate the identified memory block with a first portion of a first file to which the identified memory block is mapped at a first time and a checksum representing data within the identified memory block at the first time;

determine whether the identified memory block is mapped to the first portion of the first file at a second time subsequent to the first time; and

based at least in part on determining that the identified memory block is mapped to the first portion of the first file at the second time, indicate that the checksum represents expected data within the identified memory block.

12. A system in accordance with Claim 11, wherein the processor is further programmed to associate the identified memory block with a second portion of a second file to which the identified memory block is mapped at the second time when the identified memory block is not mapped to the first portion of the first file at the second time.

13. A system in accordance with Claim 11, wherein the processor is further programmed to indicate that the checksum does not represent expected data within the identified memory block when the identified memory block is not mapped to the first portion of the first file at the second time.

14. A system in accordance with Claim 11, wherein the processor is further programmed to determine whether the identified memory block is mapped to the first portion of the first file at the second time by, at least in part, determining whether the identified memory block is allocated to operating system kernel text.

15. A system in accordance with Claim 11, further comprising a storage device coupled to at least one of the processor and the memory device, wherein the processor is further programmed to identify the identified memory block by identifying a page of virtual memory corresponding to a first memory location within the memory device, the first memory location corresponding to a second memory location within the storage device.

16. A system in accordance with Claim 15, wherein the storage device is configured to store the first file.

17. A system in accordance with Claim 11, wherein the processor is further programmed to:

determine whether a write operation corresponding to the first file has been executed between the first time and the second time; and

indicate that the checksum represents expected data within the identified memory block based in part on determining that no write operations corresponding to the first file have been executed between the first time and the second time.

18. A system in accordance with Claim 17, wherein the processor is further programmed to determine whether a write operation corresponding to the first file has been executed between the first time and the second time by comparing a first write count associated with the first file at the first time with a second write count associated with the first file at the second time.

19. A system in accordance with Claim 11, wherein the processor is further programmed to:

determine whether a write operation corresponding to the first file is pending at the second time; and

indicate that the checksum represents expected data within the identified memory block based further on determining that no write operations corresponding to the first file are pending at the second time.

20. One or more computer-readable storage media having computer-executable components for verifying an integrity of a memory device using at least one processor coupled to the memory device, the components comprising:

a control component that when executed by the at least one processor causes the at least one processor to:

identify a memory block corresponding to at least one memory location within the memory device;

a fingerprinting component that when executed by the at least one processor causes the at least one processor to:

associate the identified memory block with a first portion of a first file to which the identified memory block is mapped at a first time and a first checksum representing data within the identified memory block at the first time; and

determine whether the identified memory block is mapped to the first portion of the first file at a second time; and

a result component that when executed by the at least one processor causes the at least one processor to:

calculate a second checksum representing data within the identified memory block at the second time when the identified memory block is mapped to the first portion of the first file at the second time; and

indicate whether the second checksum is equal to the first checksum.

FIG. 1

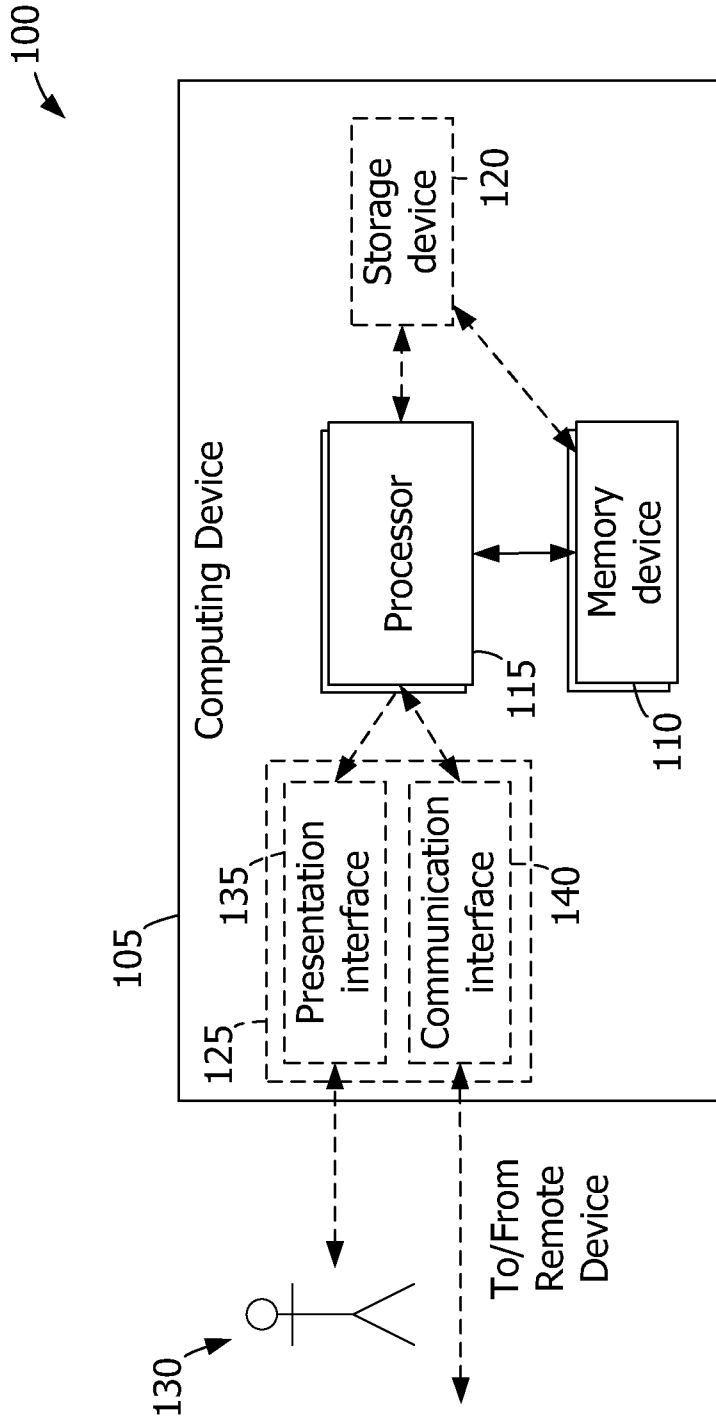




FIG. 3

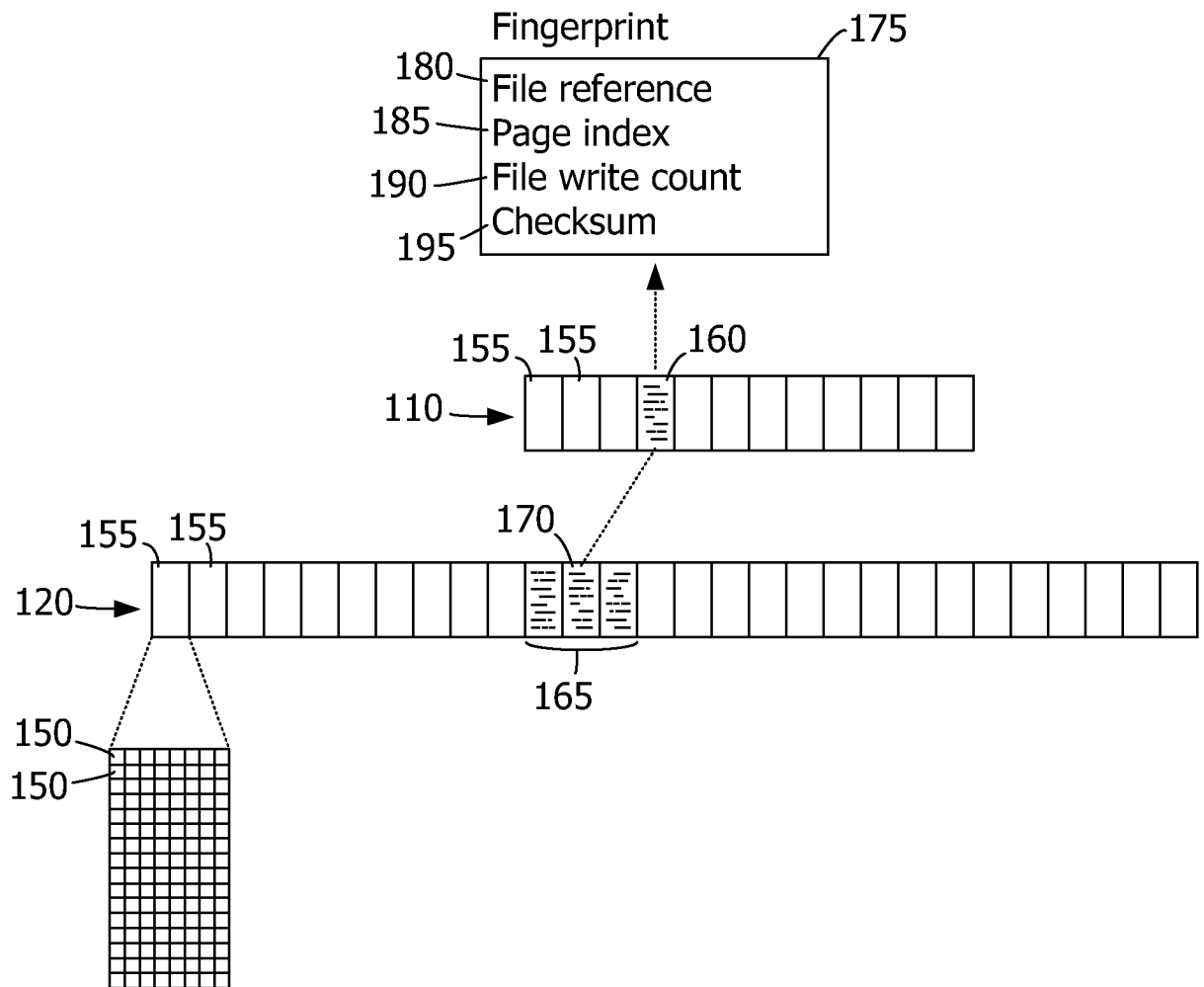


FIG. 4

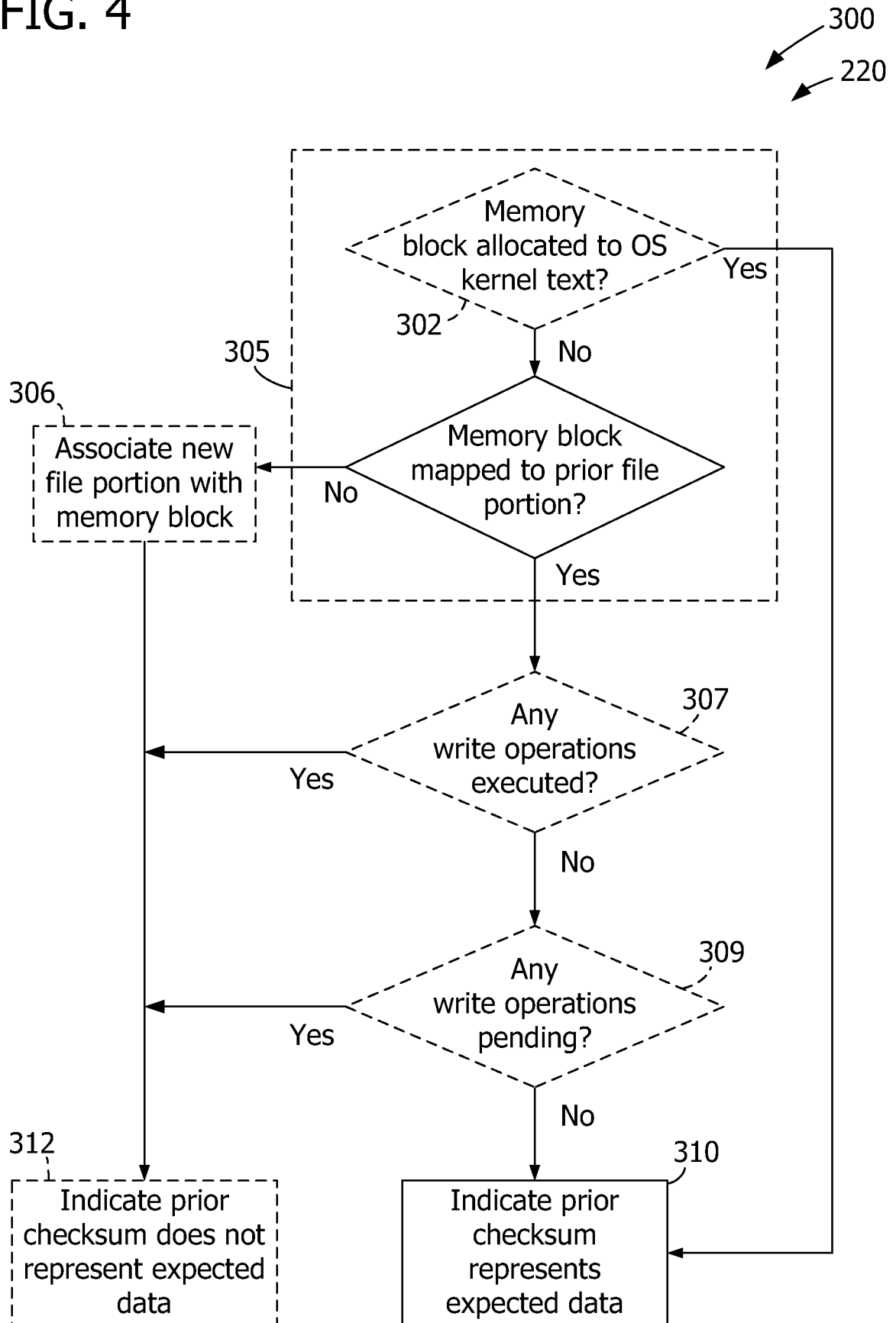


FIG. 5

