FORM 2

THE PATENTS ACT, 1970

(39 of 1970)

&

THE PATENTS RULES, 2003

COMPLETE SPECIFICATION

(See Section 10; rule 13)

Title of the Invention

SYSTEM AND METHOD FOR ANALYSING SLACK SPACE

APPLICANTS:

Name in Full	Country of Residence	Address of the Applicant
Cialfor Research Labs Pvt Ltd	India	ODC-4, 4th Floor, Panchshil Tech Park, Hinjewadi Phase 1, Pune–411057, Maharashtra, India
Quantum University	India	Quantum University, Roorkee-247167, Uttarakhand, India

The following specification particularly describes the invention and the manner in which it is performed.

TECHNICAL FIELD

The present disclosure relates generally to computer forensics and more specifically relates to performing computer forensics by analyzing slack space in a computer.

BACKGROUND ART

[0001] Since the dawn of time, humans have felt the need to conceal information, and in response to that desire, numerous techniques have been created, some of which are more successful than others. Since the invention of computers, more efficient techniques have been developed, like concealing data in a file's slack space.

[0002] Analyzing hidden files plays a crucial role in computer forensics. Computer forensics allows for analyzing for files deleted by the user while using the computer. The deleting of files does not really delete them but rather move them from one location to another location. Thus, if any movement of data is detected, potential clues can be provided to the investigators concerning the data erased by legal suspects on the hard drive

[0003] Nowadays, there are techniques that exists which are. For example, reference can be made to US7970216B2 which discloses techniques for reducing storage space instead of decompressing data. Further, the reference can be made to US9165051B2 which discloses detecting data classes in data streams. However, none of the cited references disclose techniques for analyzing slack space and determining various parameters from the analyzed slack space.

OBJECTS OF THE INVENTION

[0004] The principal object of the present invention is to provide techniques for analyzing slack space in a computer.

[0005] Another object of the present invention is to provide techniques for determining hidden files in a slack space of a computer.

[0006] Another object of the present invention is to determining malicious code in a slack space of a computer.

[0007] Another object of the present invention is to provide techniques for allowing users to locate deleted files from a memory.

SUMMARY OF THE INVENTION

[0008] In one embodiment, a system for analysing slack space is disclosed. The system comprises a memory (102), wherein the memory comprises a data region (202) configured to store user data, a slack space (204) configured to store leftover data. The system further comprises a processor (104) configured to analyse slack space to determine hidden space in the slack space.

[0009] In another embodiment, a method for analysing slack space (204) is disclosed. The method comprises providing a memory (102); wherein the memory comprises a data region and a slack space, the data region (202) stores user data and the slack space (204) stores leftover data. The method further comprises providing a processor (104) for analysing slack space to determine hidden space in the slack space.

BRIEF DESCRIPTION OF DRAWINGS

[0010] Figure 1 illustrates an apparatus for analyzing slack space, in accordance with one embodiment of the present invention.

[0011] Figure 2 illustrates a slack space, in accordance with one embodiment of the present invention.

[0012] Figure 3 illustrating a flowchart of a method for analyzing slack space, in accordance with the present invention.

DETAILED DESCRIPTION OF THE INVENTION

[0013] While the present invention is described herein by way of example using embodiments and illustrative drawings, those skilled in the art will recognize that the invention is not limited to the embodiments of drawing or drawings described and are not intended to represent the scale of the various components. Further, some components that may form a part of the invention may not be illustrated in certain figures, for ease of illustration, and such omissions do not limit the embodiments outlined in any way. It should be understood that the drawings and the detailed description thereto are not intended to limit the invention to the particular form disclosed, but on the contrary, the invention is to cover all modifications, equivalents, and alternatives falling within the scope of the present invention as defined by the appended claim.

[0014] As used throughout this description, the word "may" is used in a permissive sense (i.e. meaning having the potential to), rather than the mandatory sense, (i.e. meaning must). Further, the words "a" or "an" mean "at least one" and the word "plurality" means "one or more" unless otherwise mentioned. Furthermore, the terminology and phraseology used herein are solely used for descriptive purposes and should not be construed as limiting in scope. Language such as "including," "comprising," "having," "containing," or "involving," and variations thereof, is intended to be broad and encompass the subject matter listed thereafter, equivalents, and additional subject matter not recited, and is not intended to exclude other additives, components, integers, or steps. Likewise, the term "comprising" is considered synonymous with the terms "including" or "containing" for applicable legal purposes. Any discussion of documents, acts, materials, devices, articles, and the like are included in the specification solely for the purpose of providing a context for the present invention. It is not suggested or represented that any or all these matters form part of the prior art base or were

common general knowledge in the field relevant to the present invention.

[0015] In this disclosure, whenever a composition or an element or a group of elements is preceded with the transitional phrase “comprising”, it is understood that we also contemplate the same composition, element, or group of elements with transitional phrases “consisting of”, “consisting”, “selected from the group of consisting of, “including”, or “is” preceding the recitation of the composition, element or group of elements and vice versa.

[0016] The present invention is described hereinafter by various embodiments with reference to the accompanying drawing, wherein reference numerals used in the accompanying drawing correspond to the like elements throughout the description. This invention may, however, be embodied in many different forms and should not be construed as limited to the embodiment set forth herein. Rather, the embodiment is provided so that this disclosure will be thorough and complete and will fully convey the scope of the invention to those skilled in the art. In the following detailed description, numeric values and ranges are provided for various aspects of the implementations described. These values and ranges are to be treated as examples only and are not intended to limit the scope of the claims. In addition, several materials are identified as suitable for various facets of the implementations. These materials are to be treated as exemplary and are not intended to limit the scope of the invention.

[0017] Referring to **FIG. 1**, an apparatus 100 for analyzing slack space is disclosed. The apparatus 100 comprises a memory 102, a processor 104, an input unit 106 and a display unit 108. The processor 104 is coupled to the memory 102, the input unit 106 and the display unit 108. In one embodiment, the processor 104 may control all the operations of the various hardware/software present in the apparatus 100. The apparatus 100 may be any computing device having a slack space such as a computer, a laptop, etc.

[0018] The input unit 106 may be one or more devices for receiving input in the apparatus 100. For example, in one embodiment, the input unit 106 may be a

keyboard having various keys for receiving inputs from one or more users. Similarly, the display unit 108 may be a display screen of the apparatus 100 which may be responsible for presenting output to the one or more users. The display screen may have different sizes.

[0019] The memory 102 is a non-volatile memory where user data may be stored permanently. In one embodiment, the memory 102 may be a magnetic storage medium for the apparatus 100. The non-volatile memory is a memory which can retain user data even when the power from it has been removed. The memory 102 may have different capacities for storing data in it. In one embodiment, the memory 102 may be a hard-disk. In one embodiment, hard disks are flat circular plates made of aluminum or glass and coated with a magnetic material.

[0020] The memory 102 is partitioned into two regions- data region and slack region. This is shown in **FIG. 2**. Thus, referring to FIG. 2 now, the memory 102 is shown as been partitioned into two regions- the data region 202 and the slack space 204. In one embodiment, the data region 202 is a storage region of the hard disk. The data region 202 may be responsible for storing user data. For example, the data region 202 may be responsible for storing user personal files or folders.

[0021] The slack space 204 is the leftover storage that exists in memory 102 of the apparatus 100. In one embodiment, the slack space 204 may be stored on a computer's hard disk drive when a computer file does not need all the space it has been allocated by the operating system. For example, the computer file has been allocated with 10GB of space but the computer file needs only 5GB of the space. The examination of slack space is an important aspect of computer forensics.

[0022] To understand why slack space 204 plays an important role in E-discovery, one must first understand how data is stored on computers that have hard disk drives. Computers with hard disk drives store data in a sealed unit that contains a stack of circular, spinning disks called platters 206. Each platter 206 is composed of logically defined spaces called sectors 208 and by default, most operating system (OS) sectors are configured to hold no more than 512 bytes of

data. If a text file that is 400 bytes is saved to disk, the sector 208 will have 112 bytes of extra space left over. When the computer's hard drive is brand new, the space in a sector 208 that is not used – the slack space 204 – is blank, but that changes as the computer gets used.

[0023] When a file is deleted, the operating system doesn't erase the file, it simply makes the sector 208 occupied available for reallocation. Should a new file that is only 200 bytes be allocated to the original sector, the sector's slack space will now contain 200 bytes of leftover data from the first file in addition to the original 112 bytes of extra space. That leftover data, which is called latent data or ambient data, can provide investigators with clues as to prior uses of the computer in question as well as leads for further inquiries. For example, if a user deleted files that filled entire memory 102, and then saved new files that only filled half of the memory 102, the latter half would not necessarily be empty. It may include leftover information from the deleted files. In 2016, for example, the Federal Bureau of Investigation (FBI) revealed that it had reviewed millions of e-mail fragments that resided in the slack space of former Secretary of State Hillary Clinton's personal servers in order to determine whether or not the servers have improperly stored or transmitted classified information.

[0024] Technically, a file's slack space 204 is the difference between its logical and physical size. The logical size of a file is determined by the file's actual size and is measured in bytes. The physical size of a file is determined by the number of sectors that are allocated to the file. In most operating systems, including Windows, sectors are clustered in groups of four by default which means that each cluster has 2,048 bytes.

[0025] The logical size of the file below is 1280 bytes. This file was allocated a cluster of four 512-byte sectors, which means the physical size of the file is 2,048 bytes. The difference between 2,048 and 1,280 is 768, which means that the file's slack space is 768 bytes.

[0026] In one embodiment, an independent file blockmap (BMAP) tool is present

in the slack space 204. The BMAP is a data hiding tool that can utilize slack space in blocks to hide data. It can perform lots of functions interesting to the computer forensics community and the computer security community. BMAP has concealed and analyses the sectors and cluster data overwritten present or deleted. A directory and its subdirectories can be examined for files that have information in their slack space in addition to this basic feature and can also reveal the hidden data. It also tells if in hidden data any malicious code is there or not if there it will delete it.

[0027] Referring to **FIG. 1** again, the processor 104 may access the slack space 204 and analyze the slack space 204. The processor 104 is configured to analyze the slack space 204 of the memory 102. The processor 104 analyzes the sector and data present in the memory 102 and identify information relating to the hidden data in the slack space 204. In one embodiment, the processor 104 analyzes hidden data and show what data is overwritten and what all is present in disk.

[0028] In one embodiment, a plug and play hardware device may be provided in the apparatus 100. The plug and play hardware device do not require any installation. In one embodiment, the plug and play hardware is a universal serial bus (USB) connector. Thus, the present invention is easy to use as it provides portability and USB connector will automatically run without giving instruction and analyze to give accurate results.

[0029] The present invention allows for investigating the memory 102 to identify hidden files. Further, the present invention provides for most prevalent benefit occurs in the computer forensics field, as file slack allows users to locate files deleted from sectors. Deleting computer files doesn't fully delete them – it just moves them. This provides investigators potential clues concerning the data erased by legal suspects on the hard drive.

[0030] The techniques disclose in the present invention is operating system (OS) Independent, i.e., it does not dependent on which operating system is running on the apparatus 100. The present invention can solve two purposes- inform about

hidden data as well as present the hidden data to the users/network administrator. The present invention also helps provide information about the malicious code if any and try to delete it and increases your performance.

[0031] Referring to FIG. 3 now, a flowchart of a method 300 for analyzing slack region is provided. At step 302, the method comprises partitioning memory of the apparatus into data region and slack space. At step 304, the method comprises analyzing the slack space to detect determining hidden files in a slack space. At step 306, the method comprises analyzing the slack space to determine malicious code in the slack space. At step 308, the method comprises allowing users to locate deleted files in the slack space.

[0032] The various actions, acts, blocks, steps, or the like in the flow diagram may be performed in the order presented, in a different order or simultaneously. Further, in some embodiments, some of the actions, acts, blocks, steps, or the like may be omitted, added, modified, skipped, or the like without departing from the scope of the invention.

[0033] Although particular embodiments of the invention have been described in detail for purposes of illustration, various modifications and enhancements may be made without departing from the spirit and scope of the invention.

I/We Claim:

1. A system (100) for analysing slack space (204) comprising:
   a memory (102); wherein the memory comprises:
   a data region (202) configured to store user data;
   a slack space (204) configured to store leftover data,
   a processor (104) configured to analyse slack space to determine hidden space in the slack space.

2. The system as claimed in claim 1, wherein the processor (104) is configured to determine malicious code in the slack space (204).

3. The system as claimed in claim 1, wherein the processor (104) is configured to locate hidden files in the slack space (204).

4. The system as claimed in claim 1, wherein the user data is personal data of a user.

5. The system as claimed in claim 1, wherein the processor (104) is configured to present hidden files to a user.

6. A method for analysing slack space (204), the method comprising:
   providing a memory (102); wherein:
   the memory comprises a data region and a slack space
   the data region (202) stores user data;
   the slack space (204) stores leftover data,
   providing a processor (104) for analysing slack space to determine hidden space in the slack space.

7. The method as claimed in claim 6, wherein the processor (104) is configured to determine malicious code in the slack space (204).

8. The method as claimed in claim 6, wherein the processor (104) is configured to locate hidden files in the slack space (204).

9. The method as claimed in claim 6, wherein the user data is personal data of a user.

10. The method as claimed in claim 6, wherein the processor (104) is configured to present hidden files to a user.

Dated this: 23rd Sept, 2022

Name:
TAPASYA DUA
IN-PA/1634

ABSTRACT

SYSTEM AND METHOD FOR ANALYZING SLACK SPACE

A system and a method for analysing slack space (204) are disclosed. The system comprises a memory (102), wherein the memory comprises a data region (202) configured to store user data, a slack space (204) configured to store leftover data. The system further comprises a processor (104) configured to analyse slack space to determine hidden space in the slack space.

[Figure 1]