Techniques in Computer Forensics: A Recovery Perspective

Bhanu Prakash Battula prakashbattula@yahoo.com
Lecturer, Department of Information Technology
V.R Siddhartha Engineering College
Vijayawada, AndhraPradesh, India.

B. Kezia Rani prajayrathan@gmail.com
Asst. Professor, Dept. of Computer Science
Adi Kavi Nannaya University
Rajahmundry, Andhra Pradesh, India

R. Satya Prasad profrsp@gmail.com
Professor, Department of Computer science and Engineering
Acharya Nagarjuna University
Guntur, Andhra Pradesh, India

T. Sudha thatimakula_sudha@yahoo.com
Professor, Dept. of Computer Science
Sri Padmavathi Mahila Viswavidhyalayam
Tirupati, Andhra Pradesh, India

ABSTRACT

Computer forensics has recently gained significant popularity with many local law enforcement agencies. It is currently employed in fraud, theft, drug enforcement and almost every other enforcement activity. The research paper includes the types of attempts to destroy or tamper the files by the culprits and unleashes various recovery techniques, and their significance in different situations from those attempts, which destroy files or inflict physical damage to the computer. The paper also presents the nature and immediate need of enhancing the existing automated forensics tools. The paper gives a quick glance of various methods used by culprits to destroy the information in the electronic storage media and their corresponding forensic approach done by the computer forensic experts in the perspective of recovery.

Keywords: Computer Forensics, NiFe alloy, fraud, disks.

1. INTRODUCTION

Forensic technologies are designed to prepare and extract evidence from a seized computer system. The basic method of preserving, detecting and obtaining the electronic evidences was described in [1], [2]. This extraction is performed in such a manner to satisfy the requirements of the courts [14], [17]. Typically, the data that resides on the fixed drive of a system has been erased or otherwise altered in order to protect incriminating information. Forensic technologies make it possible to retrieve such altered data.

The origin of computer forensics can perhaps be traced back to a collection of intelligent tools. The primary focus of which was to address the problem of espionage. In recent years this problem has escalated dramatically primarily due to advances in electronic information storage.

Information in an electronic format is extremely easy to extract and store**.** Volumes of printed matter can be retrieved in an insignificant amount of time and stored on a small 3.5-inch disk.

In contrast to standard recovery procedures, forensics extracts information in a manner that meets the requirements of the courts. In order for evidence to stand in court an exact procedure for extraction must be followed. This evidence must be produced in a strict and demanding format.

2. WORKING DEFINITION OF COMPUTER FORENSICS

The term *computer forensics* has many synonyms and contexts. It originated in the late 1980s with early law enforcement practitioners [15] who used it to refer to examining standalone computers for digital evidence of crime. Some prefer it to call it as *media analysis*. Some have argued that forensic computing is a more accurate term, especially because digital evidence is increasingly captured from objects not commonly thought of as computers (such as digital cameras). Despite this one can use the generic term *computer forensics*.

Dictionaries associate the term “forensic” as obtaining evidence “suitable for the courts or public debate” included in this definition is the process of obtaining knowledge by exposing “rudimentary” evidence or the “most elementary level”. These concepts are consistent with the practices of popular forensic professions. In this profession, the term forensics implies the use of tools to present some aspect of evidence not available through standard observation. It is also recognized that the act of obtaining evidence does not necessarily constitute a forensic act. For example, concluding a blood stained knife identified at the crime scene as the weapon for doing the crime will not be a forensic activity rather it should be derived or concluded from the matching attributes of blood stains of both the knife’s and the victim’s apparel by conducting appropriate chemical tests. Similarly concluding a bullet came from a gun by observing the gun when it is shot is a conclusion not derived from forensics. Matching the microscopic groves on a bullet to the barrel of the gun does employ forensic principles. In both the above cases the latter comprises evidence found on the most elementary level while the former does not.

It follows that standard file copy programs or routines that search for text do not operate as forensic tools. In the case of programs designed to move data from one place to another, new evidence is not uncovered. Procedures executing a text search are also disqualified since they can be accomplished by standard observation. The reconstruction of files by uncovering patterns of bytes, or obtaining data from a microscopic view of a medium’s magnetic domains does serve as suitable candidates for forensic research.

Similarly, data manipulation along with other processes that transform information in some fashion cannot be considered as forensic operations. Examples include encryption, data compression and other types of encoding. These methods are only used to transform the same evidence into a different form and do not serve to uncover new evidence. Despite the fact that in a transformed format this type of evidence is not readily understood, it is readily observable and hence does not qualify. Furthermore, the operations on this evidence are not performed on an elementary level but rather on a higher level comprised of characters and text files. These endeavors more appropriately belong to the field of cryptology. An individual skilled in the field of cryptology need not employ an understanding of computer fundamentals in order to perform these operations.

A working definition of Computer Forensics can be formulated as the pursuit of knowledge by uncovering elemental evidence extracted from a computer in a manner suitable for court proceedings [3]. The term *elemental* implies operations on a fundamental level; such as the microscopic elements of the medium or the bits and bytes of an individual sector. The term *uncover* refers to the presentation of some aspect of evidence not available through simple observation.

3. TYPES OF ATTEMPTS IN DESTROYING FILES

Modern computer hard drives contain an assortment of data, including an operating system [8][10], application programs, and user data stored in files. Drives also contain backing store for virtual memory, and operating system's meta information, such as directories, file attributes, and allocation tables [8]. Drives include directory blocks, startup software (boot blocks, virgin blocks that were initialized at the factory but never written).

Level	Where found	Description
Level 0	Regular files	Information contained in the file system. Includes file names, file attributes, and file contents. One can directly access them.
Level 1	Temporary files	Temporary files, including print spooler files, browser cache files, files for "helper" applications, and recycle bin files. Most users either expect the system to automatically delete this data or are not even aware that it exists. Note: level 0 files are a subset of level 1 files.
Level 2	Deleted files	When a file is deleted from a file system, most operating systems do not overwrite the blocks on the hard disk that the file is written on. Instead, they simply remove the file's reference from the containing directory. The file's blocks are then placed on the free list. These files can be recovered using traditional "undelete" tools, such as Norton Utilities.
Level 3	Retained data blocks	Data that can be recovered from a disk, but which does not obviously belonged to a named file. Level 3 data includes information in slack space, backing store for virtual memory, and level 2 data that has been partially overwritten so that an entire file cannot be recovered. A common source of level 3 data is disks that have been formatted with Windows Format command or the Unix *newfs* command. Even though the output of these commands might imply that they overwrite the entire hard drive, in fact they do not, and the vast majority of the formatted disk's information is recoverable with the proper tools. Level 3 data can be recovered using advanced data recovery tools that can "unformat" a disk drive or special-purpose forensic tools.
Level 4	Vendor-hidden blocks	This level consists of data blocks that can only be accessed using vendor-specific commands. This level includes the drive's controlling program and blocks used for bad-block management.
Level 5	Overwritten data	Many individuals maintain that information can be recovered from a hard drive even after it is overwritten. We reserve level 5 for such information.

TABLE 1: Hierarchy of files

The most common ways of damaging hard drives include:

- Physically destroying the drive, rendering it unusable.
- Degaussing the drive to randomize the magnetic domains-most likely rendering the drive unusable in the process.
- Overwriting the drive's data so that it cannot be recovered.

We have created a hierarchy of files and their scope that reside on the disk for discussion on destruction (by culprits) and recovery (by forensic experts) presented in table 1 as a part of forensic analysis.

3.1 Destroying files through erasing

In [13], Anthony Verducci states three methods of destroying files via.

- File by file method (Individual files eliminated, software remains intact)
- Thewhole-drive method (Entire drive is permanently erased, but stil usable)
- The power tool method (Data is gone, hard drive is toast)

In most cases culprits use the *delete* and *erase* commands to erase the files. Although the precise notion of erase depends on the file system used, in most cases, deleting a file most often merely rewrites the metadata that pointed to the file, but leaves the disk blocks containing the file's contents intact.
Consider the FAT system [9]. There are four slightly different versions of this study: FAT12, FAT16, VFAT, and FAT32. A hard disk is always addressed in terms of 512 byte sectors. A FAT file system further groups data sectors into clusters that consist of 2^i sectors where 'i' is a parameter set when the drive is formatted. Each hard-disk cluster has an entry in the FAT that describes its status. The cluster is either

- Part of a file, and points to the next cluster of that file
- The last cluster in a file, and thus holds a special end-of-file (EOF) value
- Free, and thus zero
- Marked defective

Essentially, the FAT is a linked list of clusters that correspond to files. When operating system erases a FAT file, two things occur. First, the system modified the filename's first character in the file's directory entry to signal that the file is deleted and that the directory entry can be recycled. Second, the system moves all of the file's FAT clusters to the hard drive's list of free clusters. The actual file data is never touched.

3.2 Destroying files through overwriting

Every computer storage device contains files (used space) and free space (unused space). Each time the computer is used it may modify the metadata of the files in the used space and may overwrite previously deleted data that exists in the unused space [12].

Deleting files using *delete* or *erase* commands denote the low-level expertise of the individual. But expert culprits follow the destruction through overwriting so that the original data cannot be recovered.
One-way they follow to overwrite a hard disk is to fill every addressable block with ASCII NUL bytes (zeroes). If the disk drive is functioning properly, then each of these blocks reports a block filled with NULs on read-back.

Sanitization is a technique for erasing/deleting sensitive information, or to increase the free space in the disk and therefore erasing of files sometimes can be referred as Sanitization of disk. It is obvious that deletion done by an unauthorized individual is a criminal activity. There is a possibility of using potential sanitization tools by the attackers/culprits to destroy the files of authorized individuals.

4. TECHNIQUES TO RECOVER

The tools, techniques and methodologies of electronic investigation, gathering and analysis have been tried and proven and are accepted in many countries [18]. While recovering the data the integrity of the original media must be maintained through out the entire investigation [16]. The basic methods of recovering unrecoverable data are described in [7], [19]. The forensic analysis tools are used for recovering hard-disk information. Forensic tools analyze hard disks or hard-disk images from a variety of different operating systems and provide an Explorer-style interface so that one can read the files. The international important forensic tools [4] are presented in table 2:

Tool	Platform	Nature
Drivespy [22]	DOS/Windows	Inspects slack space and deleted file metadata.
Encase [21]	Windows	Features sophisticated drive imaging and preview modes, error checking, and validation, along with searching, browsing, time line, and registry viewer. Graphical user interface. Includes hash analysis for classifying known files.
Forensic [23] Tool kit	Windows	Graphic search and preview of forensic information, including searches for JPEG images and Internet text.
I Look [25]	Windows	Handles dozens of file systems. Explorer interface to deleted files. Generates hashes of files. Filtering functionality. This tool only available to US government and law enforcement agencies.
Norton Utilities	Windows	Contains tools useful for recovering deleted files and sector-by-sector examination of a computer's hard disk
The Coroner's tool kit [26]	Unix	A collection of programs used for performing post-mortem forensic analysis of Unix disks after a break-in
XWays [20]	Windows	Disk Cloning and Imaging, Native support of NTFS, FAT, Ext2/3/4, CDFS, UDF, Complete access to disks, RAIDs, and images more than 2 TB in size, Various data recovery techniques and file carving, Gathering slack space, free space, inter-partition space, and generic text from drives and images, and Mass hash calculation for files (CRC32, MD4, ed2k, MD5, SHA-1, SHA-256, RipeMD, etc.).
TASK [24]	Unix	Operates on disk images created with dd. Handles FAT, FAT32, and toolkit. Analyzes deleted files and slack space, and includes time-line NTFS, Novel, Unix, and other disk formats. Built on Coroner's Toolkit.

TABLE 2: List of Forensic tools

Many of these forensic tools can find " undeleted" files (level 2 data) and display hard-drive information that is no longer associated with a specific file (level 3 data). Using certain vendor-specific disk-drive commands level 4 information can be recovered.
The challenges that are categorized in the level 5 are:

- Magnetic alteration
- Physically damaging the drive
- Overwritten data

Physical damage to a computer or even to the hard drive itself may render the drive inoperable. Although a drive may be dented, the disk contained inside is often found to be intact. Even physical damage to the disk does not necessarily prevent recovery. Data contained on a disk that has been physically cut into pieces has been successfully recovered.

4.1 Magnetic alteration

Thomas E Dinan et. al did significant work on the magnetic media. In [11], they have stated that the magnetic poles of the disk head are formed with a magnetized ferro material (NiFe alloy) having a graduated composition in which a higher Fe concentration is fabricated proximate the write gap layer between the magnetic poles, and each magnetic pole is fabricated in a single electroplating step in which the duty cycle of the electroplating current is altered during the electroplating operation. Increase in the duty cycle implies Fe ion concentration is likewise greatest shown in figure 1.

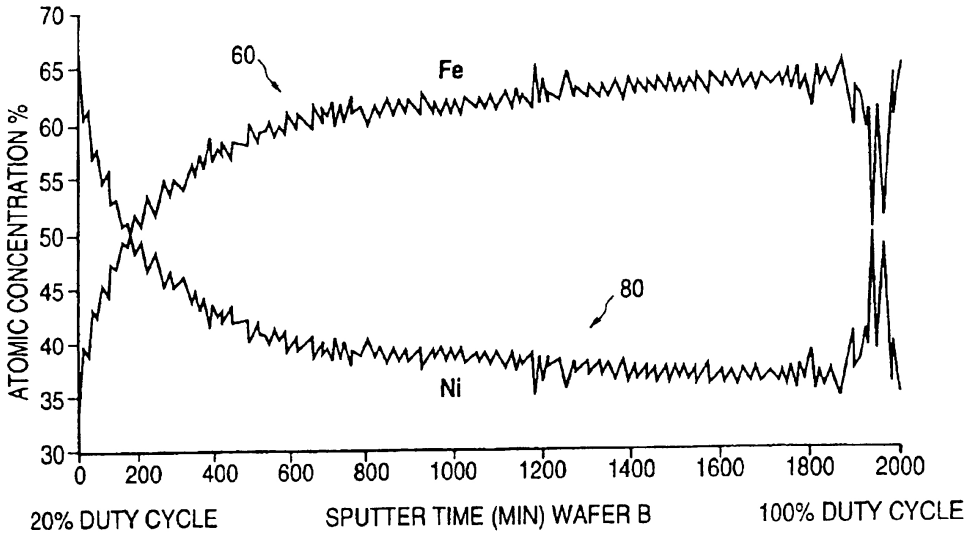

FIGURE 1: Atomic concentration of Fe, Ni in a magnetic disk

Altering the file information recorded in the Directory and FAT typically erases files. The FAT determines the next group of sectors in a file. When this information is lost, another means must be developed to find the next sector(s) in a file. The next consecutive sector is the first candidate to be examined. If this sector does not belong to the file then other factors are examined. In the case of a text file, options are needed to provide the operator a means to input the next word or group of letters that would occur at the start of the next sector. An intelligent routine has the ability to recognize which sectors of a file belong together. For example within a text file a word or phrase may end prematurely at the end of the current sector and is continued on to the next. The next sector can reside anywhere on the disk. The intelligent routine automatically searches for the sector that begins with the missing characters and links it to the recovered file.

Sector format is also examined. For example, the embedded command characters that are used to set up the margins headers and other parameters of the file can identify a sector belonging to a document file. If a sector does not contain these characteristics, it is not likely that it belongs to the file. Once a sector is found that meets all the criteria, it is linked to the recovered file. Attempt to render the drive inoperable are typically directed at the Boot and Partition sectors. Determining and recording the parameters of the drive can construct a new Boot sector. The recovery of the Partition Table requires a more elaborate procedure. A popular place to store sensitive information is on a secondary or virtual drive. The Partition Table identifies where these secondary drives are located. The quick destruction of the Partition Table is the preferred method for keeping this sensitive information from being discovered. When the Partition Table is destroyed, access to the secondary drives is lost. It is an extremely time consuming process to

locate these drives manually. By employing an intelligent search, a forensic system is able to quickly find the lost partition thus restoring access to the lost information.

A search for FATs and Boot sectors pose a more difficult problem since they are composed of numeric entries with a large range of correct values. Here it is necessary to perform an intelligent search. The parameters obtained from the sector must be weighted against the general characteristics of the drive. For example, if the boot sector indicates that there are a certain number of sectors per cluster and the location of files are arranged in a manner to suggest otherwise, this particular value can be concluded to be unreasonable. The procedure is then to extract a particular piece of information, then performing the necessary tests to verify whether the value is reasonable. The FAT or Boot Sector is found when it is determined that all the values in a given sector are reasonable.

4.2 Physical damage

The magnetic layer that contains data is only about 1 micro inch. If the disk is bent so that the head can no longer fly there is no documented method for commercial viable recovery. At times external repairs can be made to the drive to restore operation. Some circuitry and at times the stepper motor can be replaced without entering the interior areas of the drive. More extensive repair requires that the magnetic disks be removed and placed in an operational drive. This procedure requires special equipment and the most pristine of environments (Note: the driver companies do not supply the spare parts). Because of the close tolerances of the drive, any contaminants could easily destroy the surface of the disk. Thus the operations are performed in a “clean room”. Actually the clean room usually consists of two rooms. The first is a “holding” or “scrubbing” room designed to remove contaminates brought in by visitors. While an air purification system is removing particles from the body, a special mat serves to removes dirt from shoes.

In the main room another air is purifier is at work to further clean the air. Once the environment is pronounced clean, the drive can be opened and work can be performed on the disks. Repairs are now made to the magnetic disks if necessary. The disks are then installed into a functioning drive.

4.3 Overwritten data

Magnetic media is composed of small weak domains in which all of the magnetic moments are aligned in one direction. A domain acts a weak magnet aligned in some random direction. The overwritten data can be depicted in figure 2.

Consider the surface of a disk drive upon which information has not yet been recorded. As the drives magnetic head passes over the medium, the domains align underneath its surface. The area located a short distance away from the head generation the field is referred to as the fringe area. Although the magnetic field is weaker in the fringe area, it is strong enough to convert a smaller weaker domain into one that is strong.

When the head passes over the media a second time, the magnetic field produced underneath the head is strong enough to change the domains orientation. However, the field generated in the fringe areas does not possess the strength to alter the fringe domains. Thus in an ideal case, the original information remains in the fringe area. The domains of the fringe areas are translated to bits, which are in turn assembled to form data elements.

It is not necessary to observe the magnetic domains directly. The most straightforward method is to align a modified head and circuitry in order to track a fringe area and read the information in the normal fashion. Domain condition may be ascertained by the strength and form of the signal.

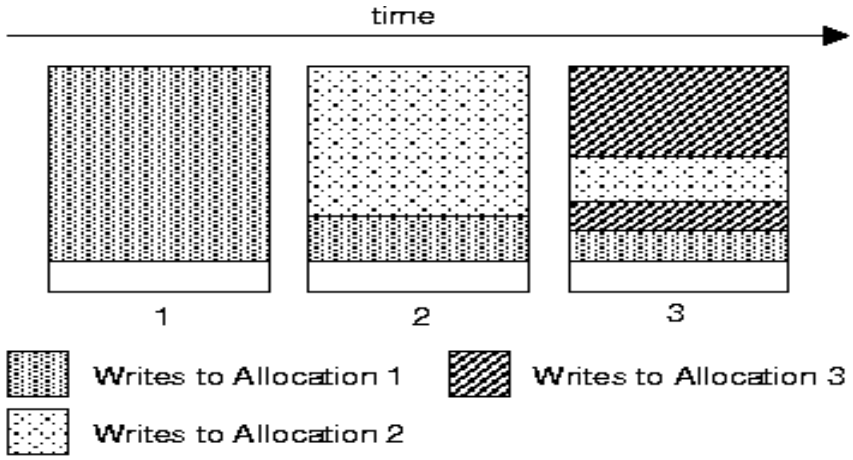

FIGURE 2: Method of overwritten data

5. CONCLUSION & FUTURE WORK

The existing automated forensic tools play vital role in the aspect of recovery. Each forensic tool has its own limitations and constraints. The existing tools show little effort to recover the file when the disk is magnetically altered and/or physically damaged and/or overwritten, by the experienced culprits. Hence there is an urgent need to enhance the automated tools with the above-discussed techniques to make the computer forensic analysis a full pledged and legally valid.

6. REFERENCES

1. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, Computer Crime and Intellectual Property Section (CCIPS) July-2002. http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm

2. Thomas Welch, "*Handbook of information Security Management"*, CRC Press LLC, 1999.

3. G.Shpantzer and T.Ipsen, "*Law Enforcement Challenges in Digital Forensics*." Proc. 6th National Colloquium Information System Security Education. NCISSE Colloquium press, 2002.

4. Simson L. Garfinkel and Abhi Shelat, "*Remembrance of Data Passed: A Study of Disk Sanitization Practices*", IEEE Security & Privacy, Vol. 1, 2003, pp. 17-27.

5. M. Villano, "*Hard-Drive Magic: Making Data Disappear Forever*", New York Times, 2, May 2002.

6. S.Berinato, "Good Stuff Cheap", CIO, 15 Oct.2002 pp 53-59.

7. Charles H Sobey, "*Recovering unrecoverable data*", Channel Science white paper, 14th April 2004.

8. Peterson, Siberschaz, Galvin, "*Secondary Storage Structure, Advanced Operating Systems*", 6th Edition.

9. Guy Hart-Davis,"*Windows(R) XP Professional: The Complete Reference"* McGraw-Hill Osborne, Dec. 2002.

10. Andrew S.Tanenbaum, "*Modern Operating Systems*" Prentice Hall, Dec. 2007.

11. Dinan, Thomas Edward, Robertson, Neil Leslie, Tam, Alan Jun-yuan, "*Magnetic head for hard disk drive having varied composition nickel-iron alloy magnetic poles*", U.S. Patent No. 6,912,771. July 5, 2005.

12. Michele C. S. Lange, Kristin M. Nimsger, ''*Electronic evidence and discovery*", American Bar Association, 2004.

13. Anthony Verducci, "*How to Absolutely, Positively Destroy Your Data*": DIY Tech, February 2007. http://www.popularmechanics.com/technology/how_to/4212242.html

14. Nelson, Bill, Philips, Amelia, Enfinger, Frank and Stewart, Chris, "*Guide to Computer Forensics and Investigations*", Thomson, Cousre Technology, Boston, 2004.

15. http://www.computerforensics.net/forensics.htm

16. Thomas Rude CISSP, "*Evidence Seizure Methodology for Computer Forensics*". http://www.crazytrain.com/seizure.html.

17. http://www.forensics.com

18. Wofle, Henry B, *Computers and Security*, El sevier Science, Ltd, pp. 26-28. http://www.sciencedirect.com

19. David Icove, Karl Seqer, William Von Storch, "*Computer crime: A Crime-figher's Handbook*", O'Reilly Media, Inc, USA (1 Aug 1995).

20. http://www.x-ways.net/forensics/index-m.html.

21. http://en.wikipedia.org/wiki/EnCase.

22. http://www.digitalintelligence.com/software/disoftware/drivespy/

23. www.accessdata.com

24. www.sleuthkit.org/

25. www.forensicswiki.org/wiki/ILook

26. www.porcupine.org/forensics/tct.html