ISSN:2229-6093

Identification and Analysis of hard disk drive in digital forensic

Kailash Kumar
Phd(CSE) Student
PEC University of Technology
kumar21002002@yahoo.com

Dr. Sanjeev Sofat
Prof. and Head CSE Deptt.
PEC University of Technology
sanjeevsofat@pec.ac.in

Dr. Naveen Aggarwal
Asst. Prof. CSE Deptt.
UIET, Punjab University
navagg@gmail.com

ABSTRACT

The dramatic increase in crime relating to the Internet and computers has caused a growing need for computer forensics. Computer forensic tools have been developed to assist computer forensic investigators in conducting a proper investigation into digital crimes. Digital forensics is a growing and important fields of research for current intelligence, law enforcement, and military organizations today. As more information is stored in digital form, the need and ability to analyze and process this information for relevant evidence has grown in complexity. Digital Forensics helps this information for analyzing and evaluating digital data as evidence. The practice of digital forensics is new. When computers became common in homes and businesses, the police more and more often came across computers which contained forensic evidence. This paper focuses on the identification and analysis of hard disk drive in digital forensics examination.

Keywords: Digital forensics, HDD, PDA

1.INTRODUCTION

The field of digital forensic analysis has experienced rapid growth in recent years, as the use of computer forensic analysis proved invaluable in a wide range of legal proceedings. Digital forensics is used not only to investigate computerized crimes, such as network intrusion, fabrication of data and illegitimate material distribution through digital services, but also to investigate crime where evidence is stored in any digital format on any digital device. Compounding with the increased usage and collection of digital evidence is the rapidly increasing storage capacity of media such as hard disks (Turner, 2005). The rapid expansion in storage requirements is not confined to the field of forensics, with modern data reduction and de-duplication techniques widely deployed in primary enterprise storage applications.

This paper explains the importance of the information that exists in hard disk drive for forensic analysis and investigations. The contribution of the paper is mainly twofold: a) a systematic method for finding fingerprints of identification of hard disk drive. b) the most important one is a extracting sensitive information for analysis,

The remainder of this paper is organized as follows. Section 2 gives an overview of the hard disk drives. Section 3 provides a short background on digital forensics. Section 4 focuses on forensic analysis process model for extracting sensitive information from hard disk drive. Finally section 5 concludes the paper and our future work.

2.HARD DISK DRIVES - THE BASICS

Despite the phenomenal increase in mobile devices such as mobile phones and PDAs over recent years, the hard disk drive (or just "hard disk" or "hard drive") remains the most common focus of computer forensic investigation. In many ways, the basic design of the hard disk has changed very little since its introduction, although changes to individual components have brought about remarkable improvements in speed, capacity and reliability. Exposing the internal architecture of a typical hard disk drive contains the four major components as described briefly over here. They are the Disk Platter, Head Arm, the Chassis, and the Head Actuator. The Chassis is the part of the hard disk that acts as the base and provides the physical support to it. The Chassis is the part of the hard disk drive over which the other parts are placed.

2.1PLATTERS

Platters are the circular disks located one above the other and mounted on a central pole known as a spindle. The platters are specially coated on each side with a coating which enables them to store data in magnetic form. Data is stored in concentric circles on both upper and lower surfaces of the platter and these circles are referred to as tracks. Each track is divided into individual sections called sectors when a disk is powered on and the system needs to read or write data the platters spin at a very high speed (driven by the spindle motor) which enables the correct part of the disk to be read through use of the actuator arm and the components associated with it.

2.2 ACTUATOR ARM (OR ACTUATOR ASSEMBLY OR HEAD ASSEMBLY)

In order to actually read data from or write data to a disk (i.e. to or from a platter) a tiny device called a read/write head needs to be positioned just above the platter surface. In order to position the head correctly it is located on the end of a "head arm" (strictly speaking, the read/write head is attached to a "head slider" which itself is attached to the head arm). The number of head arms present in a hard disk is determined by the number of platters with each arm usually being used to position a read/write head on either side of a platter. Head arms are joined together in a structure referred to as an actuator arm, actuator assembly or head assembly. In order to position the read/write heads in the correct place on the platters the assembly pivots on an axis which allows the heads to move across the platter surface. This action, together with the rotation of the platter itself, allows the heads to be positioned correctly.

2.3 HARD DRIVE TECHNICAL SPECIFICATIONS PARAMETERS

Form factor	Width	Height	Largest capacity	Platters (Max)
3.5″	102 mm	25.4 mm	3 TB (2010)/4 TB Prototype (2011)	5
2.5″	69.9 mm	7–15 mm	1.5 TB (2010)	4
1.8″	54 mm	5, 8 mm	320 GB (2009)	3

Table1. Current hard disk form factors

Form factor	Width	Largest capacity	Platters (Max)
5.25″ FH	146 mm	47 GB (1998)	14
5.25″ HH	146 mm	19.3GB (1998)	4
1.3″	43 mm	40 GB (2007)	1
1″ (CFII/ZIF/IDE-Flex)	42 mm	20 GB (2006)	1
0.85″	24 mm	8 GB (2004)	1

Table2. Obsolete hard disk form factors

2.4 UNDERSTANDING HARD DISK PERFORMANCE IN FORENSIC APPLICATIONS

The sequential nature of forensic imaging also largely eliminates the benefits of fast interface transfer rates and large on-disk cache buffers. Even experienced forensic practitioners are often fooled by claims of high interface transfer rates, so we will spend some time discussing the difference between media transfer rate and interface transfer rate.

Interface	Peak Data Rate (bits/sec)	Peak Data Rate (bytes/sec)
IDE UDMA 5	-	100 Mbytes/sec
IDE UDMA 6	-	133 Mbytes/sec
SATA I	1.5 Gbits/sec	150 Mbytes/sec
SATA II	3.0 Gbits/sec	300 Mbytes/sec
eSATA	Same as SATA I or II	Same as SATA I or II
Ultra SCSI 320	-	320 Mbytes/sec
FireWire400 (1394A)	400 Mbits/sec	40 Mbytes/sec
FireWire800 (1394B)	800 Mbits/sec	80 Mbytes/sec
USB 2.0	480 Mbits/sec	48 Mbytes/sec

Table3. Peak Interface Transfer Rates for Selected Interface Technologies

Common hard disks today employ the SATA (Serial ATA) interface standard. As shown in Table 1, SATA I offer an interface transfer rate of 1.5Gbit/sec and SATA II offers an interface transfer rate of 3.0Gbit/sec. To those not familiar with the difference between media transfer rate and interface transfer rate, these numbers make it seem like a SATA I drive should be able to transfer data at 150MB/sec or a SATA II drive should be able to transfer data at 300MB/sec.

3.DIGITAL FORENSICS

The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations. In 2001, the Digital Forensics Research Workshop [DFRW] [8] proposed a process for digital investigations that involves the following six steps.

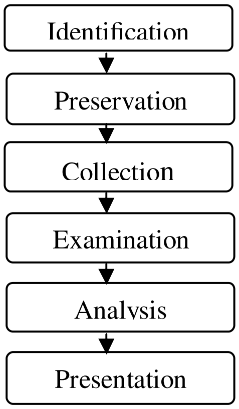


Fig1. Digital forensic investigation process

Digital forensics is the science of identifying, extracting, analyzing and presenting the digital evidence that has been stored in the digital electronic storage devices to be used in a court of law [1, 2, 3]. While forensic investigation attempts to provide full descriptions of a digital crime scene, in computer systems, the primary goals of digital forensic analysis are fivefold: i) to identify all the unwanted events that have taken place, ii) to ascertain their effect on the system, ***iii) to acquire the necessary evidence to support a lawsuit***, iv) to prevent future incidents by detecting the malicious techniques used and v) to recognize the incitement reasons and intendance of the attacker for future predictions [2,4]. The general component in digital forensic process are; acquisition, preservation, and analysis [5].

Digital electronic evidence could be described as the information and data of investigative value that are stored by an electric device, such evidence [6]. Data can be recovered even if deleted from a user's point of view. Techniques for recovery of deleted information are therefore central to digital forensics. Digitally stored information can easily be manipulated, so great care has to be taken when handling digital evidence, in order to be able to prove the origin of the information. This research focuses on the above mentioned ***third goal*** of acquiring the necessary evidence of suspect hard disk that take place on a computer system.

4.FORENSIC ANALYSIS PROCESS

In this section, we describe the forensic analysis process we had adopted to achieve the above mentioned objectives of this research work. We conducted an empirical study using selected digital forensic tools that are predominantly used in practice. Since each utility does some specific functionality, a collection of such tools were necessary to perform a comprehensive set of functionalities. Hence, the following forensic utilities / tools were adopted to conduct the experimental investigation in this research work:

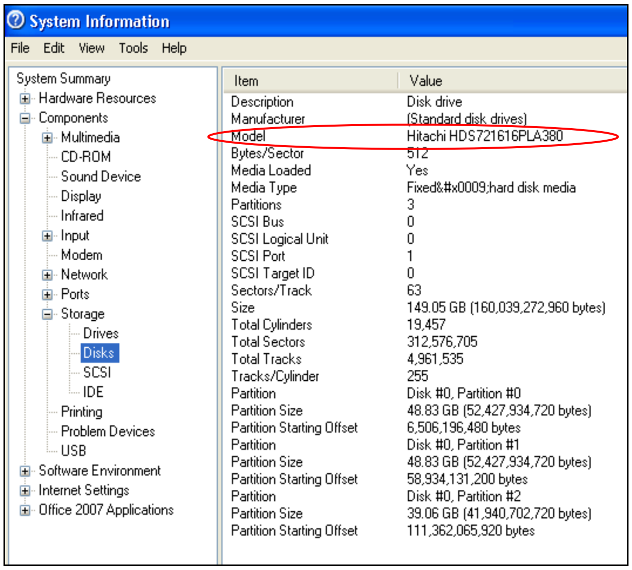
In an investigation, the analysis phase is the one that most relies on the investigator's skills and experience. To analyze the data collected about a case, an investigator wants to understand and know where the suspect might have hidden the data and in what formats and what application he might have used. Some patterns in the data are important; once found and fully examined; they can lead to more evidence. In order to achieve a successful analysis, many tools are adopted to aid investigators analyze the collected data. Common tools include **EnCase** [9] and the **Forensic ToolKit** [7] which comes with a searching tool **dtSearch**. These tools display the files of a storage media and allow the user to navigate through the files similar to traditional file explorers. However, they provide additional features that are useful in forensics context such as displaying file headers and opening compressed files. Some of these tools provide more contextual analysis features such as queries and a time-line view of the files. However, the investigator is responsible for manually performing the analysis and gathering knowledge from the extracted data.

4.1 DISK IDENTIFICATION

In some cases, if the accused has denied that the evidence presented in front of judiciary is not belonging from his/her hard drive. There are various tools available for hard disk identification in freeware, we can download and run in the accused hard drive but, it may change the hard drive integrity value. For these we have proposed some operating system utility in window environment and hardware analysis (BIOS) to retrieve hard drive identification information from accused computer without affecting the original hard drive attributes.

Step 1: System information (BIOS): The basic input/output system (BIOS) software is built into the PC, and is the first code run by a PC when powered on ('boot firmware'). The primary function of the BIOS is to set up the hardware and load and start an operating system. When the PC starts up, the first job for the BIOS is to initialize and identify system devices such as the hard disk drive, video display card, keyboard, mouse, optical disc drive and other hardware. The BIOS software provides useful information of hard disk drive such as serial no., vendor name, and capacity for identification purpose.

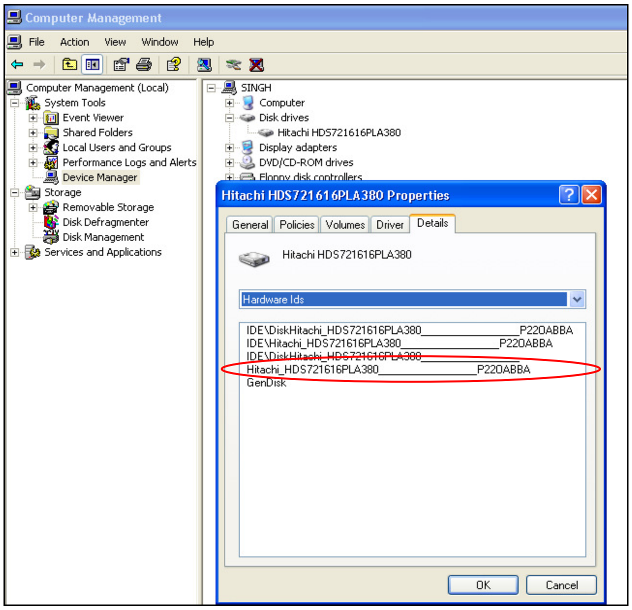
Step 2: Operating System (msinfo32.exe) MSINFO32 displays a comprehensive view of hardware, system components, and software environment of accused computer. This tool display all system information such as installed devices, drivers, CPU, BIOS, RAM, Display, Hard Disks, Removable media and much more information you can find out without changing system and drive integrity.



Item	Value
Description	Disk drive
Manufacturer	(Standard disk drives)
Model	Hitachi HDS721616PLA380
Bytes/Sector	512
Media Loaded	Yes
Media Type	Fixed&#x0009;hard disk media
Partitions	3
SCSI Bus	0
SCSI Logical Unit	0
SCSI Port	1
SCSI Target ID	0
Sectors/Track	63
Size	149.05 GB (160,039,272,960 bytes)
Total Cylinders	19,457
Total Sectors	312,576,705
Total Tracks	4,961,535
Tracks/Cylinder	255
Partition	Disk #0, Partition #0
Partition Size	48.83 GB (52,427,934,720 bytes)
Partition Starting Offset	6,506,196,480 bytes
Partition	Disk #0, Partition #1
Partition Size	48.83 GB (52,427,934,720 bytes)
Partition Starting Offset	58,934,131,200 bytes
Partition	Disk #0, Partition #2
Partition Size	39.06 GB (41,940,702,720 bytes)
Partition Starting Offset	111,362,065,920 bytes

Fig2. System Information Tool – Storage Hard Disk

Step 3: The device manager utility also plays an important role to fetch information of all hardware connected to the computer as storage devices, network adapter, modem etc., go to disk drives option and click on properties and go to the details you can find the serial no. of the hard disk connected to that system.



```
IDE\DiskHitachi_HDS721616PLA380________________P220ABBA
IDE\Hitachi_HDS721616PLA380________________P220ABBA
IDE\DiskHitachi_HDS721616PLA380________________
Hitachi_HDS721616PLA380________________P220ABBA
GenDisk
```

Fig3. Computer management- disk drives

The above mentioned method is mainly focus to provide identification information of hard drive of accused before retrieving any valuable information for law enforcement using forensic imaging tools such as EnCase or FTK. This precious information can be used in front of court of law for supportive evidence.

4.2 DISK ANALYSIS

Now, we adopted the following three stages to perform digital forensic analysis in a comprehensive manner:

Stage 1: Hard disk data acquisition: The first step in this investigative process is to acquire the evidence. The goal is to obtain an exact replica of the data without compromising its integrity; however, because computer systems may contain volatile data in RAM, the acquisition process is a dynamic one. We will assume that we are only interested in files that are known to have been created and stored on the crime suspect's hard drive. For this purpose we are using Windows® based forensic data acquisition and analysis tool EnCase Forensic Edition Version 4.

Stage 2: Evidence authentication: In this stage the investigator has to search and authenticate the evidence. The aim is to verify the integrity of the digital evidence. In other words, this procedure is necessary to prove that the data is exactly the replica as the original created at that time and date stamps of the acquired data match that of the original. A cryptographic technique called a hash is used as "a sort of electronic fingerprint for an individual file or even an entire hard drive." (kruse, p. 13) The EnCase for DOS utility provides the option of creating an MD5 hash value of the evidence at the time of acquisition. This hash value is of the newly created drive image. For evidentiary purposes, it is critically important that this hash value exists. Without it, there is no proof that the acquired image is an exact match of the original hard drive

Stage 3: Evidence Analysis: During the analysis phase of the investigation, EnCase allows the investigator to create a hash value for any file. Since the hash value is determined by the file's contents, any change to the file or timestamp results in a mismatch with any future MD5 hash value. Mismatched hash values strongly imply that the file has been modified either intentionally or unintentionally. It is also important to note that a hash value cannot be generated on a partial file; therefore, if a deleted file has been partially overwritten, an MD5 hash value for that incomplete file is not available.

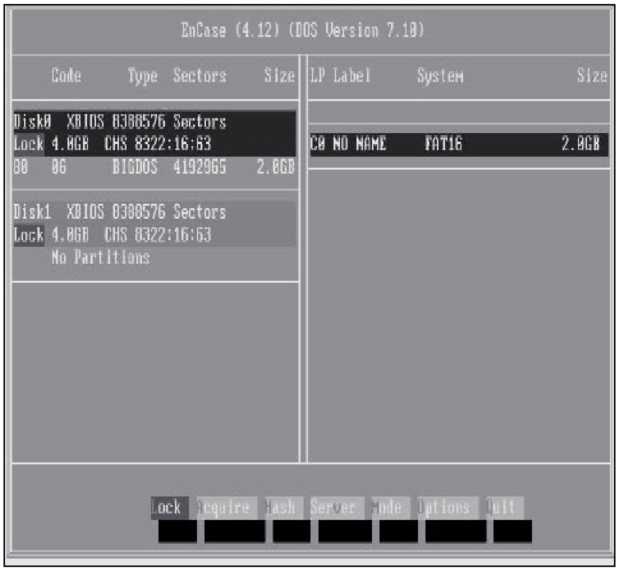
For the experimental investigation of the effectiveness of the above tools, we created test data on a Pentium (R) Core (TM) 2 Due CPU, 1.89 GHz, 0.99 of RAM with Windows XP professional. The next two steps involved for imaging digital evidence from suspect hard disk drive, for analysis and examination purpose:

Step 1: Power down the Suspect System: Powering down the suspect system allows you to state on the record and in your documentation that you've established a time and date upon which no other modifications will occur in the system. It is important that you are able to prove that nothing you do in the course of your collection, analysis, and reporting modifies the original evidence. Look inside the system to determine what drive(s) exist and remove them, even if they are not currently attached to any cabling.

Step 2: Forensically Image the Drive with an EnCase DOS Boot Disk: Here we create an EnCase DOS boot disk using the EnCase program. If you do not have an image for the EnCase DOS boot disk, you can download it. Guidance Software offers boot disks that you can download at www.guidancesoftware.com/support/downloads.shtm (under the Drivers section).

1. Choose Tools | Create Boot Disk in EnCase and follow the prompts.
2. Power down the system.
3. Reattach the suspect drive to the system.

4. Boot up the system using the EnCase DOS boot disk; depending on the version of EnCase you're using, you will either go directly into EnCase for DOS or to the command prompt. At the command prompt, enter **en** and press return.
5. Unlock the disk to which you will be writing the image of the suspect drive by highlighting Lock, pressing enter, and choosing the disk drive to unlock (in this case, we're unlocking Disk1), as shown here:



```
                 EnCase (4.12) (DOS Version 7.10)
     Code      Type  Sectors    Size | LP Label      System          Size

Disk0  XBIOS 8388576 Sectors         |
Lock 4.0GB  CHS 8322:16:63           | C0 NO NAME    FAT16          2.0GB
80   06     BIGDOS  4192965    2.0GB |

Disk1  XBIOS 8388576 Sectors         |
Lock 4.0GB  CHS 8322:16:63           |
     No Partitions                   |
```

Fig3. EnCase DOS Version interface

6. Your screen should now look like the following illustration, with the suspect drive (Disk1) shown as locked and the drive to which you want to write the image (Disk0) unlocked.
7. Select Acquire and choose the suspect drive (Drive1). You can move between options by pressing the tab key. After you have selected the suspect drive, press enter.
8. Provide the path to the directory on the image drive to which you want the image of the suspect drive to be written and the name of the image file, and then press enter. Before you choose OK, make sure that the drive you are writing to is FAT16 or FAT32, as DOS cannot read from or write to drives of other file systems. You must also make sure that enough free space is available on the destination drive to hold the image. The image will always be about 2K larger than the suspect drive for case-specific information EnCase stores in the file, so never try to image a suspect drive to another drive of the same or a smaller size without using compression.

5.CONCLUSION & FUTURE WORK

In this paper we have mentioned some technique which can help to identify the suspect hard disk before analysis of digital evidence. Once gathered, the information is then prepared it for law enforcement agencies. Our proposed method aims to address two problems: the first task to identify the suspect's hard drive, through the use of system BIOS and operating system tools. Second, task to analyze digital evidence from hard disk drive with the help of digital forensic imaging tool EnCase DOS Boot Disk. Some data mining technique such as name entity association, text summarization and image association can be applied for analysis of suspect's hard disk drive for future work.

ACKNOWLEDGMENT

The authors thankful to Mr. Amandeep Jindal, Project Assistant PEC university of Technology, Chandigarh, for their useful suggestion and hardware support for this research paper.

REFERENCES

[1] M. Reith, C. Carr, & G. Gunsch: *An examination of digital forensic models*, International Journal of Digital Evidence, 1, pp. 1-12 (2002).

[2] M. Alazab, S. Venkatraman & P. Watters: Digital *forensic techniques for static analysis of NTFS images*, Proceedings of ICIT2009, Fourth International Conference on Information Technology, IEEE Xplore (2009).

[3] B. Carrier: *File system forensic analysis*, Addison-Wesley Professional, USA, (2008). [4] S. Ardisson: Producing a Forensic Image of Your Client's Hard Drive? What You Need to Know, Qubit, 1, pp. 1-2 (2007).

[4] S. Ardisson: *Producing a Forensic Image of Your Client's Hard Drive? What You Need to Know*, Qubit, 1, pp. 1-2 (2007).

[5] M. Andrew: *Defining a Process Model for Forensic Analysis of Digital Devices and Storage Media*, Proceedings of SADFE2007, Second International Workshop on Systematic Approaches to Digital Forensic Engineering, pp. 16-30 (2007).

[6] E Investigation: *Electronic Crime Scene Investigation*: A Guide for First Responders, US Department of Justice, NCJ, (2001).

[7] AccessData Corp. Forensic toolkit (ftk). http://www.accessdata.com/forensictoolkit.html.

[8] G. Palmer. *A road map for digital forensic research*. Report From the First Digital Forensic Research Workshop (DFRWS), August 2001. http://www.dfrws.org/2001/dfrws-rm-final.pdf.

[9] Guidance Software Inc. Encase forensics. http://www.guidancesoftware.com.