Chapter 2

Computing Device Forensics

Introduction

If a digital investigator can learn about piece of hardware in a computer, hard disks are probably the best choice because they are one of the most common sources of digital evidence. This section covers hard disks basics and discusses topics that are of interest to an investigator, such as access methods, write blocking, and locations where data can be hidden.

2.1 Hard Disk Geometry & Fundamentals

Start with the internals of all modern hard disks, this information is useful for a basic understanding of how data are stored and because older file systems and partitioning schemes use disk geometry and other internal values that are hidden with modern disks. Therefore, knowing about disk geometry will help you to understand some of the values in a file system.

The goal of this section is not to enable you to fix hard disks. Instead, the goal is to obtain a conceptual understanding of what is going on inside. Hard disks contain one or more circular platters that are stacked on top of each other and spin at the same time. A picture of the inside of a disk can be found in Figure. The bottom and top of each platter is coated with a magnetic media, and when the disk is manufactured, the platters are uniform and empty.

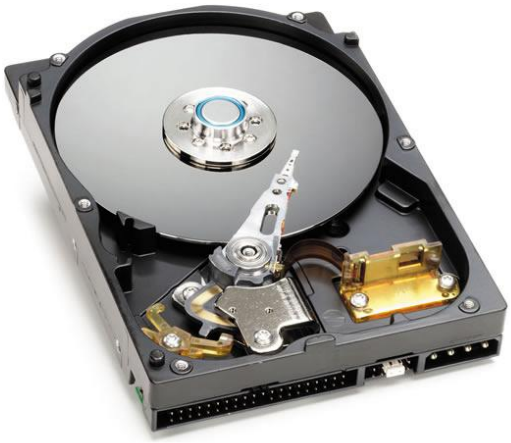


Fig: The inside of an ATA disk where we see the platters on the right and an arm on the left that reads from and writes to the platters.

Inside the disk is an arm that moves back and forth, and it has a head on the top and bottom of each platter that can read and write data, although only one head can read or write at a time.

A low-level format is performed on the blank platters to create data structures for tracks and sectors. A track is a circular ring that goes around the platter. It is similar to a lane on a running track so that if you go around the entire circle, you will end in the same location that you started. Each track on the hard disk is given an address from the outside inward, starting with 0. For example, if there were 10,000 tracks on each platter, the outside track of each platter would be 0, and the inside track (nearest the center of the circle) would be 9,999. Because the layout of each platter is the same and the tracks on each platter are given the same address, the term cylinder is used to describe all tracks at a given address on all platters.

For example, cylinder 0 is track 0 on the bottom and top of all platters in the hard disk. The heads in the disk are given an address so that we can uniquely identify which platter and on which side of the platter we want to read from or write to.

Each track is divided into sectors, which is the smallest addressable storage unit in the hard disk and is typically 512 bytes. Each sector is given an address, starting at 1 for each track.

Therefore, we can address a specific sector by using the cylinder address (C) to get the track, the head number (H) to get the platter and side, and the sector address (S) to get the sector in the track. We can see this in figure below.

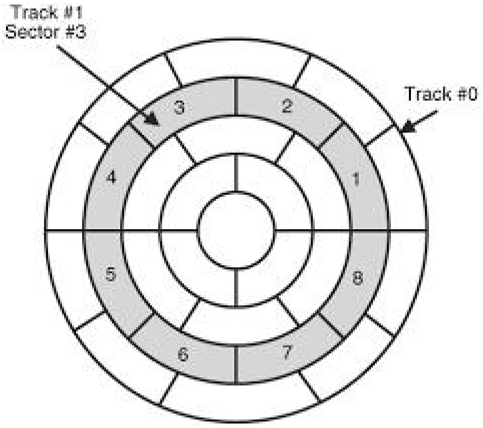


Fig: Disk geometry of one platter showing the track (or cylinder) and sector addresses (not even close to scale).

The CHS address is no longer used as the primary addressing method. The Logical Block Address (LBA) is instead used, and it assigns sequential addresses to each sector. The LBA address may not be related to its physical location.

A sector can become defective and should therefore no longer be used to store user data. With older disks, it was the responsibility of the operating system to know where the bad sectors were and to not allocate them for files. Users could also manually tell the disk which sectors to ignore because they were bad. In fact, many file systems still provide the option to mark sectors as bad. This is typically not needed, though, because modern disks can identify a bad sector and remap the address to a good location somewhere else on the disk. The user never knows that this has happened.

The previous description of the layout is overly simplified. In reality, the disk arranges the location of the sectors to obtain the best performance. So, sectors and tracks may be offset to take advantage of the seek times and speeds of the drive. For the needs of many investigators, this simplistic view is good enough because most of us do not have clean rooms, and the equipment to locate where a specific sector is located on a platter.

2.1.1 ATA / IDE Interface

The *AT Attachment* (ATA) interface is the most popular hard disk interface. Disks that use this interface are frequently referred to as IDE disks, but IDE simply stands for *Integrated Disk Electronics* and identifies a hard disk that has the logic board built into it, which older disks did not. The actual interface that the "IDE" disks use is ATA.

The ATA specifications are developed by the T13 Technical Committee (http://www.t13.org), which is a committee for the *International Committee on Information Technology Standards* (INCITS). The final version of each specification is available for a fee, but draft versions are freely available on the INCITS Web site. For the purposes of learning about hard disks, the draft versions are sufficient. ATA disks require a *controller*, which is built into the motherboard of modern systems.

The controller issues commands to one or two ATA disks using a ribbon cable. The cable has maximum length of 18 inches and has 40 pins, but newer disks have an extra 40 wires that are not connected to any pins. The interface can be seen in Figure

2.1. The extra wires are there to prevent interference between the wires. Laptops frequently have a smaller disk and use a 44-pin interface, which includes pins for power. Adaptors can be used to convert between the two interfaces, as can be seen in Figure 2.2. There is also a 44-pin high-density interface that is used in portable devices, such as Apple iPods.

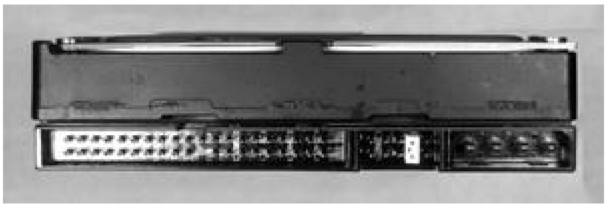


Figure 2.1 An ATA disk with the 40-pin connector, jumpers, and power connector.

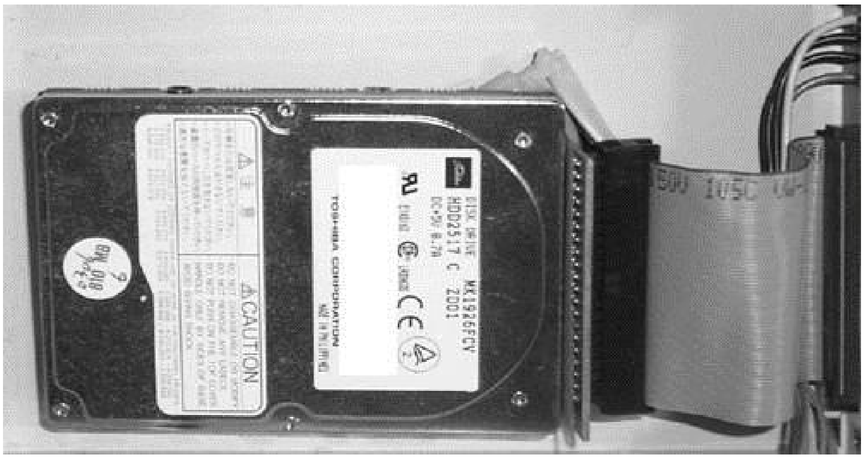


Figure 2.2. A 44-pin ATA laptop drive connected to a 40-pin ATA ribbon cable using an adapter.

The interface data path between the controller and disks is called a *channel*. Each channel can have two disks, and the terms "master" and "slave" were given to them, even though neither has control over the other. ATA disks can be configured as master or slave using a physical jumper on the disk. Some also can be configured to use "Cable Select," where they will be assigned as master or slave based on which plug they have on the ribbon cable. Most consumer computers have two channels and can support four ATA disks.

2.1.2 SCSI Drives

When building a portable incident response kit, some of the more difficult decisions may include identifying what types of *Small Computer Systems Interface* (SCSI) cables, drives, and connectors should be included. SCSI hard disks are not as common as ATA hard disks for consumer PCs, but they are standard on most servers.

Like ATA, there are many specifications of SCSI, which are published by the T10 Technical Committee for INCITS (http://www.t10.org). There are three SCSI specifications, SCSI-1, SCSI-2, and SCSI-3.

SCSI versus ATA

There are both high-level and low-level differences between SCSI and ATA. The most obvious high-level difference includes the numerous connector types. With ATA, there was only 40 and 44-pin connectors, but SCSI has many shapes and styles. The SCSI cables can be much longer than ATA cables and there can be more than two devices on the same cable.

Each device on the SCSI cable needs a unique numerical ID, which can be configured with jumpers on the disk or with software. Many SCSI disks also have a jumper to make the disk read only, which provides a similar function to an ATA write blocker. ATA write blockers are external devices that block write commands. The first low-level difference between ATA and SCSI is that SCSI does not have a controller.

The ATA interface was designed for a single controller to tell one or two hard disks what to do. SCSI was designed as a bus where different devices communicate with each other and the devices are not limited to hard disks. With a SCSI configuration, the card that plugs into the computer is not a controller because each device on the SCSI cable is essentially an equal and can make requests of each other.

Like ATA, standard SCSI is parallel and data transfers occur in 8-bit or 16-bit chunks. Also like ATA, there is a serial version of the specification, which is the serial attached SCSI specification.

2.2 Hardware & Software

Hardware

Hardware refers to the physical elements of a computer. This is also sometime called the machinery or the equipment of the computer. Examples of hardware in a computer are the keyboard, the monitor, the mouse and the processing unit. However, most of a computer's hardware cannot be seen. In other words, it is not an external element of the computer, but rather an internal one, surrounded by the computer's casing (tower). A computer's hardware is comprised of many different parts, but perhaps the most important of these is the motherboard.The motherboard is made up of even more parts that power and control the computer.

In contrast to software, hardware is a physical entity. Hardware and software are interconnected. Without software, the hardware of a computer would have no function. However, without the creation of hardware to perform tasks directed by software via the central processing unit, software would be useless.

Fig: Various Hardware

Software

Software, commonly known as programs, consists of all the electronic instructions that tell the hardware how to perform a task. These instructions come from a software developer in the form that will be accepted by the platform (operating system + CPU) that they are based on. For example, a program that is designed for the Windows operating system will only work for that specific operating system. Compatibility of software will vary as the design of the software and the operating system differ. Software that is designed for Windows XP may experience a compatibility issue when running under Windows 2000 or NT.

Software is capable of performing many tasks, as opposed to hardware which only perform mechanical tasks that they are designed for. Software is the electronic instructions that tells the computer to perform a task. Practical computer systems divide software systems into two major classes:

- **System Software:** Helps run computer hardware and computer system itself. System software includes operating systems, device drivers, diagnostic tools and more. System software is almost always pre-installed on your computer.
- **Application Software:** Allows users to accomplish one or more tasks. Includes word processing, web browsing and almost any other task for which you might install software. (Some application software is pre-installed on most computer systems.)

Software is generally created (written) in a high-level programming language, one that is (more or less) readable by people. These high-level instructions are converted into "machine language" instructions, represented in binary code, before the hardware can "run the code".

2.3 Data Storage system

Where and how data are stored and written is one of the major fundamental concepts that must be learned. There is more that one way to write data. Today, data are generally created in three different ways: electromagnetism, microscopic electrical transistors (flash), and reflecting light (CDs, DVDs, etc). Storage locations inside a computer serve different purposes. Some are for the short term, used to temporarily hold the data that the computer is using at the moment. The other is for more permanent, long-term keeping.

Magnetic Disks

Most drives in today’s computers read and write data magnetically. They will render each particle either magnetized or not magnetized. If the particle is magnetized, it’s read as a 1. If not, it’s read as a 0. The drives themselves are usually made up of aluminum platters coated with a magnetic material. These platters spin at very high speeds. The platters spin in the neighbourhood of 7,000 rpm to 15,000 rpm. The speed could even be greater for high-end drives. These heavy duty drives are typically found in servers or professional grade workstations. From a forensic standpoint, faster drive speeds can result in faster acquisitions.

Let's look at the major parts of a standard hard drive. The platters revolve around a small rod called a spindle. The data are physically written to the platter using a read/write head attached to an actuator arm, which is powered by the actuator itself. The actuator arm moves the head across the platter(s), reading and writing data. The read/write head floats on a cushion of air. The read/write head, as it's called, is barely floating above the platter surface, at a height less than the diameter of a human hair.

Fig: Inside of a Harddisk

Flash Memory

Flash memory is used in a wide range of devices. Thumb drives and memory cards provide reliable storage in a very portable package, allowing us to take more pictures and take our files on the road. Unlike other kinds of memory, flash memory retains our data even without electricity. Flash is made up of transistors. Each transistor is either carrying an electric charge or it isn't. When the transistor is charged, it is read as a "1" without a charge it's read as a "0."

Flash based hard drives are starting to become more and more common. Unlike magnetic drives, flash drives are solid state, meaning that they have no moving parts. They are often referred to as an SSD or "Solid State Drive." They offer several significant advantages including increased speed, less susceptibility to shock, and lower power consumption.

SSDs will play a major role in computing and digital forensics going forward. Although these devices offer improved performance, they also present a major challenge to digital forensics.

Optical Storage

Optical media read and write data using a laser light along with a reflective material incorporated into optical discs. Optical discs are made of a polycarbonate base covered by a thin layer of aluminium. The disc is then coated with a clear acrylic material for protective purposes. During the manufacturing process, the disc's surface is embossed with tiny bumps. This series of bumps form one long, single, spiral track. A laser projects a highly focused beam of light onto the track. The light is reflected differently from the bumps and the spaces in between, called "lands." This change in reflectivity is what the system reads as binary (Brain). The most common types of optical storage media include CDs, DVDs, and Blu-ray discs (Brain).

Volatile versus Non-volatile Memory

Memory and storage are two terms that are somewhat synonymous when it comes to computers. They both refer to internal places where data are kept. Memory is used for the short-term storage, while storage is more permanent. No matter what you call it, there is a significant difference between the two, especially from a forensic perspective. That difference lies in the data's volatility. Data in RAM exist only as long as power is supplied. Once the power is removed (i.e., the machine is turned off), the data start to disappear. This behaviour makes this kind of memory volatile. In contrast, files saved on your hard drive remain even after the computer is powered down, making it non-volatile.

RAM stores all the data that are currently being worked on by the Central Processing Unit (CPU). Data are fed from the RAM to the CPU, where they are executed. Traditionally, forensic analysis of a computer focused on the hard drive, as much of the evidence can be found there. Some instant messaging applications, for example, don't write to the hard drive unless the logging feature is turned on. AOL Instant Messenger and MSN fall into that category. So, if logging is off (which it is by default), the only evidence will be found in RAM while the machine is running.

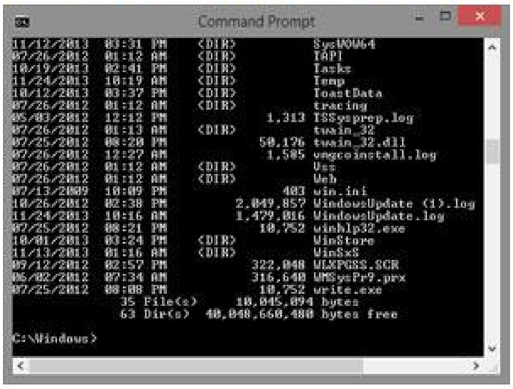
2.4 Types of OS

An operating system is the most important software that runs on a computer. It manages the computer's memory and processes, as well as all of its software and hardware. It also allows you to communicate with the computer without knowing how to speak the computer's language. Without an operating system, a computer is useless.

Your computer's operating system (OS) manages all of the software and hardware on the computer. Most of the time, there are several different computer programs running at the same time, and they all need to access your computer's central processing unit (CPU), memory, and storage. The operating system coordinates all of this to make sure each program gets what it needs.

Operating systems usually come pre-loaded on any computer you buy. Most people use the operating system that comes with their computer, but it's possible to upgrade or even change operating systems. The three most common operating systems for personal computers are Microsoft Windows, Mac OS X, and Linux.

Windows Command Prompt Window



```
11/12/2013  03:31 PM    <DIR>          SysWOW64
07/26/2012  01:12 AM    <DIR>          TAPI
10/19/2013  02:41 PM    <DIR>          Tasks
11/24/2013  10:19 AM    <DIR>          Temp
10/12/2013  03:37 PM    <DIR>          ToastData
07/26/2012  01:12 AM    <DIR>          tracing
05/03/2012  12:12 PM             1,313 TSSysprep.log
07/26/2012  01:13 AM    <DIR>          twain_32
07/25/2012  08:20 PM            50,176 twain_32.dll
07/26/2012  12:27 AM             1,505 vmgcoinstall.log
07/26/2012  01:12 AM    <DIR>          Vss
07/26/2012  01:12 AM    <DIR>          Web
07/13/2009  10:09 PM               403 win.ini
10/26/2012  02:38 PM         2,049,857 WindowsUpdate (1).log
11/24/2013  10:16 AM         1,479,016 WindowsUpdate.log
07/25/2012  08:21 PM            10,752 winhlp32.exe
10/01/2013  03:24 PM    <DIR>          WinStore
11/13/2013  01:16 AM    <DIR>          WinSxS
09/12/2012  02:57 PM           322,048 WLXPGSS.SCR
06/02/2012  07:34 AM           316,640 WMSysPr9.prx
07/25/2012  08:08 PM            10,752 write.exe
              35 File(s)     10,045,094 bytes
              63 Dir(s)  40,048,660,480 bytes free

C:\Windows>
```

2.4.1 Microsoft DOS

Short for Microsoft Disk operating system, MS-DOS is a non-graphical command line operating system derived from 86-DOS that was created for IBM compatible computers. MS-DOS originally written by Tim Paterson and introduced by Microsoft in August 1981 and was last updated in 1994 when MS-DOS 6.22 was released. MS-DOS allows the user to navigate, open, and otherwise manipulate files on their computer from a command line instead of a GUI like Windows.

2.4.2 Windows OS

Windows OS, computer operating system (OS) developed by Microsoft Corporation to run personal computers (PCs). Featuring the first graphical user interface (GUI) forIBM-compatible PCs, the Windows OS soon dominated the PC market. Approximately 90 percent of PCs run some version of Windows.

The first version of Windows, released in 1985, was simply a GUI offered as an extension of Microsoft's existing disk operating system, or MS-DOS. Based in part on licensed concepts that Apple Inc. had used for its Macintosh System Software, Windows for the first time allowed DOS users to visually navigate a virtual desktop, opening graphical "windows" displaying the contents of electronic folders and files with the click of a mouse button, rather than typing commands and directory paths at a text prompt.

Subsequent versions introduced greater functionality, including native Windows File Manager, Program Manager, and Print Manager programs, and a more dynamic interface. Microsoft also developed specialized Windows packages, including the networkable Windows for Workgroups and the high-powered Windows NT, aimed at businesses. The 1995 consumer release Windows 95 fully integrated Windows and DOS and offered built-in Internet support, including the World Wide Web browser Internet Explorer.

2.4.3 LINUX

Linux is a free and open-source operating system developed by Linus Torvalds and friends and was first announced by Linus in a post he made August 25,1991. The Linux kernel runs on numerous different platforms including the Intel and Alpha platform and is available under the GNU General Public License.

Linux may be obtained in two different ways. All the necessary components can be downloaded free of charge from the Internet. This means that an individual operating system can be assembled for almost nothing. An alternative is to use a so-called Distribution, offered by various companies and including a wide range of applications and installation programs that significantly simplify the installation of Linux.

Presently, Linux is successfully being used by several millions of users worldwide. The composition of user groups varies from private users, training companies, universities, research centers right through to commercial users and companies, who view Linux as a real alternative to other operating system.

2.4.4 MAC OS

Mac OS is a series of graphical user interface–based operating systems developed by Apple Inc. for their Macintosh line ofcomputer systems. The original operating system was first introduced in 1984 as being integral to the original Macintosh, and referred to as the "System". Referred to by its major revision starting with "System 6" and "System 7", Apple rebranded version 7.6 as "Mac OS" as part of their Macintosh clone program in 1996. The Macintosh, specifically its system software, is credited with having popularized the early graphical user interface concept.

Mac OS is a line of operating systems created by Apple. It comes preloaded on all new Macintosh computers, or Macs. All of the recent versions are known as **OS X**(pronounced O-S Ten), and the specific versions include **El Capitan** (released in 2015)**,** **Yosemite** (2014)**,** **Mavericks** (2013)**,** **Mountain Lion** (2012)**, and Lion** (2011)**.**

2.4.5 UNIX

A term coined by Brian Kernighan, Unix or UNIX (not an acronym) is an operating system that was developed by some of the members of the MULTICS team at the Bell Laboratories starting in the late 1960's, many of who also helped create the C programming language. Today, Unix is not just the work of a couple of programmers, organizations, institutes, and other individuals have contributed significant additions to Unix and its variants, making it a widely used and popular operating system.

Unix is primarily a command line oriented operating system you can get additional applications such as X-Window, which allows you to have a graphic oriented operating system similar to Windows. Since, Unix is often used from the command line there are various shells. A shell is a large add-on or modification of the Unix operating system, to determine the shell you can type echo $shell at the Unix prompt. When typing this command a response such as "/bin/csh" is displayed, which indicates you are logged into is a C shell. Bourne shell is "/bin/sh" and Korn shell which is "/bin/ks\.

2.5 Disk Forensics

Disk forensics is the science of extracting forensic information from digital storage media like Hard disk, USB devices, Firewire devices, CD, DVD, Flash drives, Floppy disks etc. The process of Disk Forensics are:

1. Identify digital evidence
2. Seize & Acquire the evidence
3. Authenticate the evidence

4. Preserve the evidence
5. Analyze the evidence
6. Report the findings
7. Documenting

Step 1: Identification of storage devices at the scene of crime like hard disks with IDE/SATA/SCSI interfaces, CD, DVD, Floppy disk, Mobiles, PDAs, flash cards, SIM, USB/ Fire wire disks, Magnetic Tapes, Zip drives, Jazz drives etc. These are some of the sources of digital evidence.

Step 2: Seizing the storage media for digital evidence collection. This step is performed at the scene of crime. In this step, a hash value of the storage media to be seized is computed using appropriate cyber forensics tool. Hash value is a unique signature generated by a mathematical hashing algorithm based on the content of the storage media. After computing the hash value, the storage media is securely sealed and taken for further processing.

One of the cardinal rules of Cyber Forensics is “Never work on original evidence”. To ensure this rule, an exact copy of the original evidence is to be created for analysis and digital evidence collection. Acquisition is the process of creating this exact copy, where original storage media will be write protected and bit stream copying is made to ensure complete data is copied into the destination media. Acquisition of source media is usually done in a Cyber Forensics laboratory.

Step 3: Authentication of the evidence is carried out in Cyber Forensics laboratory. Hash values of both source and destination media will be compared to make sure that both the values are same, which ensures that the content of destination media is an exact copy of the source media.

Step 4: Electronic evidences might be altered or tampered without trace. Once the acquisition and authentication have been done, the original evidence should be placed in secure storage keeping away from highly magnetic and radiation sources. One more copy of image should be taken and it needs to be stored into appropriate media or reliable mass storage. Optical media can be used as the mass storage. It is reliable, fast, longer life span and reusable.

Step 5: Verification of evidence before starting analysis is an important step in Cyber Forensics process. This is done in Cyber Forensics laboratory before commencing analysis. Hash value of the evidence is computed and compared it with the hash value taken at the time of acquisition. If both the values are same, there is no change in the content of the evidence. If both are different, there is some change in the content. The result of verification should be properly documented.

Analysis is the process of collecting digital evidence from the content of the storage media depending upon the nature of the case being examined. This involves searching for keywords, picture analysis, time line analysis, registry analysis, mailbox analysis, database analysis, cookies, temporary and Internet history files analysis, recovery of deleted items and analysis, data carving and analysis, format recovery and analysis, partition recovery and analysis, etc.

Step 6: Case analysis report should be prepared based on the nature of examination requested by a court or investigation agency. It should contain nature of the case, details of examination requested, details of material objects and hash values, result of evidence verification, details of analysis conducted and digital evidence collected, observations of the examiner and conclusion. Presentation of the report should be in simple terms and precise way so that non-technical persons should be able to understand the content of the report.

Step 7: Documentation is very important in every step of the Cyber Forensics process. Everything should be appropriately documented to make a case admissible in a court of law. Documentation should be started from the planning of case investigation and continue through searching in scene of crime, seizure of material objects, chain of custody, authentication and acquisition of evidence, verification and analysis of evidence, collection of digital evidence and reporting, preservation of material objects and up to the closing of a case.

2.6 Data Recovery Tools

In computing, **data recovery** is a process of salvaging inaccessible data from corrupted or damaged secondary storage, removable media or files, when the data they store cannot be accessed in a normal way. The data is most often salvaged from storage media such as internal or external hard disk drives (HDDs), solid-state drives (SSDs), USB flash drives, magnetic tapes, CDs, DVDs, RAID subsystems, and other electronic devices. Recovery may be required due to physical damage to the storage device or logical damage to the file system that prevents it from being mounted by the host operating system (OS). Below is the description of Most used Data Recovery tools.

1. Recuva

With both free and pay editions, Recuva is an incredibly powerful tool for recovering data from Linux and Window partitions. With support for all Windows versions from XP through Windows 8.1, this is a great tool to bring dead data back to life.It is able to recover files that have been "permanently" deleted and marked by the operating system as free space. The program can also be used to recover files deleted from USB flash drives, memory cards, or MP3 players.

2. Pandora Recovery

With a free version for recovering data from secondary drives, and a pay version you can put on a USB key to recover an operating system drive, Pandora Recovery has a versatile offering that can bring back most data without issue. Pandora Recovery allows us to find and recover recoverable deleted files from NTFS and FAT-formatted volumes, regardless of their type - we can recover pictures, songs, movies or documents. Pandora Recovery will scan your hard drive and build an index of existing and deleted files and directories (folders) on any logical drive of your computer with supported file format.

3. PC INSPECTOR File Recovery

PC INSPECTOR File Recovery is a great recovery tool for Windows systems. It can recognize data types even when the header is missing, so you can recover from deletions, formatting, or even total volume loss. It is a program that allows its users to recover lost data and their supporting file systems FAT 12/16/32 and NTFS under Windows (all versions including Vista). It turns out to be very effective when the boot sector (boot) or FAT is damaged or deleted.

4. TestDisk

It is a Software designed to recover lost partitions or repair drives that are no longer bootable. It can repair most file systems (NTFS, FAT, EXT) and also recover data from deleted partitions. It can run under most versions of Windows, Linux, BSD, and Mac operating systems. It also can be deployed as a bootable image to recover from unbootable systems.

5. WinHex

A multitasker that includes a disk editor, imaging software, encryption and checksumming, format converter, and more. It is more targeted towards investigation and forensics than simple data recover, and has several different levels of licensing, depending upon required features. It has an evaluation version that is free to try for as long as you need.

2.7 Open Source Tools for Investigation

1. SANS SIFT

The SANS Investigative Forensic Toolkit (SIFT) is an Ubuntu based Live CD which includes all the tools you need to conduct an in-depth forensic or incident response investigation. It supports analysis of Expert Witness Format (E01), Advanced Forensic Format (AFF), and RAW (dd) evidence formats. SIFT includes tools such as log2timeline for generating a timeline from system logs, Scalpel for data file carving, Rifiuti for examining the recycle bin, and lots more.

2. ProDiscover Basic

ProDiscover Basic is a simple digital forensic investigation tool that allows you to image, analyse and report on evidence found on a drive. Once you add a forensic image you can view the data by content or by looking at the clusters that hold the data. You can also search for data using the Search node based on the criteria you specify.

3. Volatility

Volatility is a memory forensics framework for incident response and malware analysis that allows you to extract digital artifacts from volatile memory (RAM) dumps. Using Volatility, you can extract information about running processes, open network sockets and network connections, DLLs loaded for each process, cached registry hives, process IDs, and more.

4. The Sleuth Kit (+Autopsy)

The Sleuth Kit is an open source digital forensics toolkit that can be used to perform in-depth analysis of various file systems. Autopsy is essentially a GUI that sits on top of The Sleuth Kit. It comes with features like Timeline Analysis, Hash Filtering, File System Analysis and Keyword Searching out of the box, with the ability to add other modules for extended functionality.

5. FTK Imager

FTK Imager is a data preview and imaging tool that allows you to examine files and folders on local hard drives, network drives, CDs/DVDs, and review the content of forensic images or memory dumps. Using FTK Imager, you can also create SHA1 or MD5 hashes of files, export files and folders from forensic images to disk, review and recover files that were deleted from the Recycle Bin (providing that their data blocks haven't been overwritten), and mount a forensic image to view its contents in Windows Explorer.

6. Linux 'dd'

dd comes by default on the majority of Linux distributions available today (e.g. Ubuntu, Fedora). This tool can be used for various digital forensic tasks such as forensically wiping a drive (zero-ing out a drive) and creating a raw image of a drive.

7. CAINE

CAINE (Computer Aided Investigative Environment) is Linux Live CD that contains a wealth of digital forensic tools. Features include a user-friendly GUI, semi-automated report creation and tools for Mobile Forensics, Network Forensics, Data Recovery and more.

8. Oxygen Forensic Suite 2013 Standard

If you are investigating a case that requires you to gather evidence from a mobile phone to support your case, Oxygen Forensics Suite (Standard Edition) is a tool that will help you achieve this. Features include the ability to gather Device Information (Manufacturer, OS Platform, IMEI, Serial Number, etc.), Contacts, Messages (Emails, SMS, MMS, etc.) and recovery of deleted messages, Call Logs, and Calendar and Task information. It also comes with a file browser which allows you to access and analyse user photos, videos, documents and device databases.

9. Free Hex Editor Neo

Free Hex Editor Neo is a basic hex editor that was designed to handle very large files. While a lot of the additional features are found in the commercial versions of Hex Editor Neo, this tool is useful for loading large files (e.g. database files or forensic images) and performing actions such as manual data carving, low-level file editing, information gathering, or searching for hidden data.

10. Bulk Extractor

Bulk extractor is a computer forensics tool that scans a disk image, file, or directory of files and extracts information such as credit card numbers, domains, e-mail addresses, URLs, and ZIP files. The extracted information is output to a series of text files (which can be reviewed manually or analysed using other forensics tools or scripts).

11. DEFT

DEFT is another Linux Live CD which bundles some of the most popular free and open source computer forensic tools available. It aims to help with Incident Response, Cyber Intelligence and Computer Forensics scenarios. Amongst others, it contains tools for Mobile Forensics, Network Forensics, Data Recovery, and Hashing.

12. Xplico

Xplico is an open source Network Forensic Analysis Tool (NFAT) that aims to extract applications data from internet traffic (e.g. Xplico can extract an e-mail message from POP, IMAP or SMTP traffic). Features include support for a multitude of protocols (e.g. HTTP, SIP, IMAP, TCP, UDP), TCP reassembly, and the ability to output data to a MySQL or SQLite database, amongst others.

13. Mandiant RedLine

RedLine offers the ability to perform memory and file analysis of a specific host. It collects information about running processes and drivers from memory, and gathers file system metadata, registry data, event logs, network information, services, tasks, and Internet history to help build an overall threat assessment profile.

14. HELIX3 Free

HELIX3 is a Live CD based on Linux that was built to be used in Incident Response, Computer Forensics and E-Discovery scenarios. It is packed with a bunch of open source tools ranging from hex editors to data carving software to password cracking utilities, and more.

15. USB Historian

USB Historian parses USB information, primarily from the Windows registry, to give you a list of all USB drives that were plugged into the machine. It displays information such as the name of the USB drive, the serial number, when it was mounted and by which user account. This information can be very useful when you're dealing with an investigation whereby you need to understand if data was stolen, moved or accessed.

2.9 Tools and Techniques

Tools are the predefined software or methods which are available for application of digital forensic.

The following tools are described below:

1. EnCase

EnCase is another popular multi-purpose forensic platform with many nice tools for several areas of the digital forensic process. This tool can rapidly gather data from various devices and unearth potential evidence. It also produces a report based on the evidence. This tool does not come for free.

2. The Sleuth Kit

The Sleuth Kit is a Unix and Windows based tool which helps in forensic analysis of computers. It comes with various tools which helps in digital forensics. These tools help in analyzing disk images, performing in-depth analysis of file systems, and various other things.

3. X-Ways Forensics

X-Ways Forensics is an advanced platform for digital forensics examiners. It runs on all available version of Windows. It claims to not be very resource hungry and to work efficiently. If we talk about the features, find the key features in the list below:

- Disk imaging and cloning
- Ability to read file system structures inside various image files
- It supports most of the file systems including FAT12, FAT16, FAT32, exFAT, TFAT, NTFS, Ext2, Ext3, Ext4, Next3, CDFS/ISO9660/Joliet, UDF.
- Automatic detection of deleted or lost hard disk partition
- Various data recovery techniques and powerful file carving
- Bulk hash calculation
- Viewing and editing binary data structures using templates
- Easy detection of and access NTFS ADS
- Well maintained file header
- Automated activity logging
- Data authenticity
- Complete case management
- Memory and RAM analysis
- Gallery view for pictures
- Internal viewer for Windows registry file
- Automated registry report
- Extracts metadata from various file types

- Ability to extract emails from various available email clients.

4. Forensic Tool Kit

Forensic Tool Kit is a commercial forensics tool developed by AccessData . This tool allows the CFS to view all files on the chosen storage device. A function of this tool includes immediate generation of hash values for files that are viewed within an investigation. Forensic Tool Kit does not support data recovery. Since the data discovery functionality of the tool is not effective, data analysis and recovery are both affected.

5. Foremost and scalpel:

Linux program to recover files based on their headers and footers. Can work on image files, such as those generated by *dd*, Safeback, Encase, etc, or directly on a drive. The headers and footers are specified by a configuration file, so we can pick and choose which headers we want to look for.

6. Pyflag:

PyFlag is a forensic and log analysis GUI and computer forensics framework written in python. Basically it provides features for log analysis, disk forensic and network forensic.Disk forensics - extracting forensic information from hard disk images, keyword search , MD5 hash comparison. Used in log analysis. It works as network forensic.

7. XRY

XRY is the mobile forensics tool developed by Micro Systemation. It is used to analyze and recover crucial information from mobile devices. This tool comes with a hardware device and software. Hardware connects mobile phones to PC and software performs the analysis of the device and extract data. It is designed to recover data for forensic analysis. The latest version of the tool can recover data from all kind of smartphones including Android, iPhone and BlackBerry. It gathers deleted data like call records, images, SMS and text messages.

8. Cellebrite UFED

Cellebrite's UFED solutions present a unified work flow to allow examiners, investigators and first responders to collect, protect and act decisively on mobile data with the speed and accuracy a situation demands – without ever compromising one for the other. The UFED Pro Series is designed for forensic examiners and investigators who require the most comprehensive, up-to-date mobile data extraction and decoding support available to handle the influx of new data sources. Platform agnostic, the UFED Field Series is designed to unify work flows between the field and lab, making it possible to view, access and share mobile data via in-car workstations, laptops, tablets or a secure, self-service located at a station.

2.9.1 Digital Forensic Techniques

Digital forensic techniques involve the application of science to the identification, collection, examination, and analysis of data in ways that preserve the integrity of the information and maintain a strict chain of custody for the data. Organizations have the means to collect growing amounts of data from many sources. Data is stored or transferred by standard IT systems, networking equipment, computing peripherals, personal digital assistants (PDAs), consumer electronic devices, and various types of media. When information security incidents occur, organizations that have established a capability to apply digital forensic techniques can examine and analyze the data that they have collected, and determine if their systems and networks may have sustained any damage and if sensitive data may have been compromised. Digital forensic techniques can be used for many purposes, such as supporting the investigation of crimes and violations of internal policies, analyses of security incidents, reviews of operational problems, and recovery from accidental system damage.

Below are the list of Digital Forensic Techniques:

- Recovering deleted files
- Production of time stamps and other meta data
- Removing known files
- File signatures verifications
- String searching and file fragments

- Web browsing activity reconstruction
- Email activity Reconstruction
- Microsoft Windows registry reconstruction
- Analyzing unknown files
- Alternate data streams
- Live forensics
- Recovering hidden files

2.10 Command line Tools

1. The Sleuth Kit (TSK):

The Sleuth Kit (TSK) is a popular collection of unix-based, command line forensic utilities. The Sleuth Kit (TSK) is a library and collection of command line tools that allow you to investigate disk images. The core functionality of TSK allows you to analyze volume and file system data. The plug-in framework allows you to incorporate additional modules to analyze file contents and build automated systems. The library can be incorporated into larger digital forensics tools and the command line tools can be directly used to find evidence.

Below is a description of each utility in Sleuth Kit:

A) File System Layer Tools

These file system tools process general file system data, such as the layout, allocation structures, and boot blocks.

fssstat: Shows file system details and statistics including layout, sizes, and labels.

B) File Name Layer Tools

These file system tools process the file name structures, which are typically located in the parent directory.

ffind: Finds allocated and unallocated file names that point to a given meta data structure.

fls: Lists allocated and deleted file names in a directory.

C) Meta Data Layer Tools

These file system tools process the meta data structures, which store the details about a file. Examples of this structure include directory entries in FAT, MFT entries in NTFS, and inodes in ExtX and UFS.

icat: Extracts the data units of a file, which is specified by its meta data address (instead of the file name).

ifind: Finds the meta data structure that has a given file name pointing to it or the meta data structure that points to a given data unit.

ils: Lists the meta data structures and their contents in a pipe delimited format.

istat: Displays the statistics and details about a given meta data structure in an easy to read format.

D) Data Unit Layer Tools

These file system tools process the data units where file content is stored. Examples of this layer include clusters in FAT and NTFS and blocks and fragments in ExtX and UFS.

dcat: Extracts the contents of a given data unit.

dls: Lists the details about data units and can extract the unallocated space of the file system.

dstat: Displays the statistics about a given data unit in an easy to read format.

dcalc: Calculates where data in the unallocated space image (from dls) exists in the original image. This is used when evidence is found in unallocated space.

E) File System Journal Tools

These file system tools process the journal that some file systems have. The journal records the metadata (and sometimes content) updates that are made. This could help recover recently deleted data. Examples of file systems with journals include Ext3 and NTFS.

jcat: Display the contents of a specific journal block.

jls: List the entries in the file system journal.

F) Media Management Tools

These tools take a disk (or other media) image as input and analyze its partition structures. Examples include DOS partitions, BSD disk labels, and the Sun Volume

Table of Contents (VTOC). These can be used find hidden data between partitions and to identify the file system offset for The Sleuth Kit tools. The media management tools support DOS partitions, BSD disk labels, Sun VTOC, and Mac partitions.

mmls: Displays the layout of a disk, including the unallocated spaces. The output identifies the type of partition and its length, which makes it easy to use 'dd' to extract the partitions. The output is sorted based on the starting sector so it is easy to identify gaps in the layout.

G) Image File Tools

This layer contains tools for the image file format. For example, if the image format is a split image or a compressed image.

img_stat: This tool will show the details of the image format.

img_cat: This tool will show the raw contents of an image file.

H) Disk Tools

These tools can be used to detect and remove a Host Protected Area (HPA) in an ATA disk. A HPA could be used to hide data so that it would not be copied during an acquisition. These tools are currently Linux-only.

disk_sreset: This tool will temporarily remove a HPA if one exists. After the disk is reset, the HPA will return.

disk_stat: This tool will show if an HPA exists. (Sleuth Kit Informer #17)

I) Other Tools

hfind: Uses a binary sort algorithm to lookup hashes in the NIST NSRL, Hashkeeper, and custom hash databases created by md5sum. (Sleuth Kit Informer #6)

mactime: Takes input from the fls and ils tools to create a timeline of file activity.

sorter: Sorts files based on their file type and performs extension checking and hash databse lookups. (Sleuth Kit Informer #3, #4, #5)

sigfind: Searches for a binary value at a given offset. Useful for recovering lost data structures. (Sleuth Kit Informer #17).

2. Tasklist.exe

This is a built-in tool to check all the available image name, PID session name, memory usage and session ID. To get detailed information about processes, you can use /v and /svc switch.

3. Pstools

This is a collection of useful process related tools. You can download it from http://technet.microsoft.com/en-us/sysinternals/bb896682.aspx. After downloading, unzip it in any location. Say, you have unzipped in your C drive. To run the commands, open your command prompt and then type the location of the Pstools folder. Next type the name of the exe file located in the PSToos folder.

```
C:\PSTools> pslist
```

4. Strings

The **strings** utility displays strings of printable characters found in the specified files. These strings are at least four characters long and must be terminated by a NUL character or a newline. If you specify a file name of - or no file names at all,**strings** reads the standard input. This utility finds interesting pieces of information in binary files. It is frequently used for looking through executable files to uncover copyright notices, error messages, undocumented features, and so on.

2.11 RAM Forensics

Computers require that a certain amount of computer memory called “random access memory” (RAM) be used by the operating system and its applications when the computer is in operation. The computer utilizes this RAM to write the current processes it is using as a form of a virtual clipboard. The information is there for immediate reference and use by the process. This type of data is called “volatile data” because it simply goes away and is irretrievable when the computer is off. Volatile data stored in the RAM can contain information of interest to the investigator.

This information could include, for example:

1. Running processes.
2. Executed console commands.

3. Passwords in clear text.
4. Unencrypted data.
5. Instant messages (IMs).
6. Internet Protocol (IP) addresses.
7. Trojan Horse(s).

There are other types of volatile data that could be considered evidence of interest to an investigation. This potentially exculpatory information may also simply “go away” when the system is turned off or loses power. This type of volatile data as potential evidence can also be collected from a running Microsoft Windows computer.

Some of the additional data that can be collected may include:

1. Who is logged into the system.
2. Open ports and listening applications.
3. Lists of currently running processes.
4. Registry information.
5. System information.
6. Attached devices (this can be important if you have a wireless-attached device not obvious at the crime scene).

2.12 File System

In computing, a file system is used to control how data is stored and retrieved. Without a file system, information placed in a storage area would be one large body of data with no way to tell where one piece of information stops and the next begins. By separating the data into individual pieces, and giving each piece a name, so that the information is easily separated and identified. Hence each group of data is called a "file". The structure and logic rules used to manage the groups of information and their name is called a "file system".

There are various file systems. Each one has different structure, logic, properties of speed, flexibility, security, size and many more. Some file systems have been designed to be used for specific applications. For example, the ISO 9660 file system is designed specifically for optical discs.

File systems can be used on many different kinds of storage devices. Each storage device uses a different kind of media. The most common storage device in use today is a hard drive whose media is a disc that has been coated with a magnetic film. The film has ones and zeros 'written' on it, sending electrical pulses to a magnetic "read-write" head. Other media that are used are magnetic tape, optical disc, and flash memory. In some cases, the computer's main memory (RAM) is used to create a temporary file system for short term use.

Some file systems are used on local data storage devices, others provide file access via a network protocol (for example, NFS,[2]SMB, or 9P clients). Some file systems are "virtual", in that the "files" supplied are computed on request (e.g. procfs) or are merely a mapping into a different file system used as a backing store. The file system manages access to both the content of files and the metadata about those files. It is responsible for arranging storage space; reliability, efficiency, and tuning with regard to the physical storage medium are important design considerations.

2.12.1 Need of File System

Any computer that can be used should be installed with an operating system that acts as an interface between the user and the hardware. There is also a secondary storage device in every computer over which the operating system is installed for permanent data storage. To store any data or information over the secondary storage device there should be some sort of structure that can be used to represent the data. This representation of the data over the secondary memory is called as the file system. The file system is important part in the collection of evidence. Different operating systems employ different file systems.

The most popular operating system is Windows. The file system that are used in the Windows Operating system is FAT and NTFS. A FAT stand for File Allocation Table, also FAT happens to be the most widely used file system as well. Other operating systems may have their own file systems. For example, consider the file system in the

Linux operating system. The file system of the Linux operating system is called as extended file system. It is also possible that some operating system does provide support for the other file systems. Like in case of the Linux (UBUNTU) supports windows file system.

The Windows operating system not at all capable of listing the files and data that is stored over the partition with extended file system or Linux file system. Hence for such cases there are some software that can be used overcome this limitation. The example of one such software is Partition Magic. The task of the computer forensics specialist is to have complete knowledge of all the different types of file systems that can be used in a computer system. Usually each operating system has its own file system. The importance of the file system for a computer forensics expert is because of the details that need to be examined for the collection of the data or information as the evidence. The physical representation of a file over one file system differs from that of another. The details that need to be studied are hence file system dependent.

The file system is vital as it is responsible for the storage of file permissions. The directory structure and the file structure representation plays vital role in forensics. Computer forensics professional should have the knowledge to utilize the tools effectively for the purpose of extracting the information from the encrypted files. The forensics tools that are available provide support for the easy usage of analysing the files of different operating systems.

2.12.2 Types of File Systems

File systems are classified into the following four categories:

Disk File System: A disk file system is used for storing and recovering the files on a storage device, such as hard disks, that are directly or indirectly connected to a computer. A few examples of disk file systems are FAT16, FAT32, NTFS, ext2, ISO 9660, ODS-5, and UDF.

Network File System: A network file system is a type of file system that provides access to files on other computers on a network. The file system is transparent to the user. A few examples of network file systems are NFS, CIFS, and GFS.

Database File System: Earlier file systems use a hierarchical management structure, but in the database file system, files are identified by their characteristics, like the name, type, topic, and author of the file, or similar metadata. Therefore, a file can be easily searched using SQL queries or text searches. For example, if a user needs to find the documents written by ABC, then the search string ―documents written by ABC‖ will show the results.

Special Purpose File System: A special purpose files system is a file system where the files are organized by software during runtime. This type of file system is used for various purposes, such as communication between computer processes or temporary file space. Special purpose file systems are used by file centric operating systems such as UNIX. One example in UNIX is the /proc file system, which can be used to access information about processes and other operating system features.

2.12.3 Windows File Systems

The Main Windows and DOS file systems are the following:

FAT16 (File Allocation Table): The FAT file system is a 16-bit file system that was developed for DOS and further supported by other operating systems. It consumes little memory and is simple and reliable. File names are limited to 8 characters for the name and 3 characters for the extension. Its main short comings are that it supports a maximum of 64 KB allocation units and that it becomes less efficient on partitions larger than 32 MB. Due to its limitations, it is not suitable for file servers.

FAT12: This is a version of FAT specifically designed for floppy disks.

FAT32: This is a 32-bit version of the FAT file system using smaller clusters, which results in a more efficient storage capacity. It supports drive sizes up to 2 TB. It can relocate the root directory and use the backup copy instead of the default copy. One of the main features is that it can dynamically resize a partition.

NTFS (New Technology File System): NTFS is an entirely different file system from

FAT. It provides enhanced security, file-by-file compression, quotas, and encryption. It is designed to quickly perform standard file operations such as read, write, search, and even advanced operations such as file-system recovery on very large hard disks. When a volume is formatted as an NTFS volume, the Master File table (MFT) and several system files are created. The MFT is the first file on an NTFS volume and contains information about all the files and folders on the volume. The first information is about the partition boot sector, which starts at sector zero and can be up to 16 sectors long.

Popular Linux File Systems:

The Linux operating system is a single hierarchical tree structure that represents the file system as one single entity. It supports many different file systems. It implements a basic set of common concepts that were actually developed for UNIX. Some of the Linux file system types are Minix, ISO 9660, UMSDOS, NFS, SMB, HPFS. Minix was Linux‘s first file system. Some of the more popular file systems used with Linux is as follows:

Ext (Extended File System): The ext file system was released in April 1992. It is an elaborate extension of the Minix file system. It has a maximum partition size of 2 GB and a maximum file name size of 255 characters. The ext file system removes the two major Minix limitations of a 64 MB partition size and short file names. The major limitation of this file system is that it doesn‘t support separate access, inode modification, and data modification time stamps. It keeps an unsorted list of free blocks and inodes, and the file system is also fragmented. It was soon replaced by the second extended file system.

Ext2 (Second Extended File System): The ext2 file system was introduced in January 1993. It extends the features of ext. It uses improved algorithms, which greatly enhances its speed, and it maintains additional time stamps. It maintains a special field in the superblock that keeps track of the status of the file system and identifies it as either clean or dirty. A dirty file system will automatically scan itself for errors. The maximum file size in the ext2 file system is 4 TB (1 terabyte is 1,024 gigabytes). It is portable to other operating systems because drivers and other tools exist for accessing ext2 data. Its major shortcomings are that there is a risk of file system corruption when writing to ext2 and that it is not a journaling file system.

Ext3 (Third Extended File System): The ext3 file system is a journaling version of the ext2 file system and is greatly used with the Linux operating system. It adds a journal, without which the file system is a valid ext2 file system. It can be mounted and used as an ext2 file system, and all the utilities of ext2 can be used on it.