# Computer Forensic
## Evidence Collection and Management

## Chapter 9

## Computer Systems Disk and File Structure

# Chapter Objectives

- Identify the various components of a hard drive and the structure of disk media
- Learn the differences among the numerous disk drive interfaces and functions
- Become familiar the Windows, Macintosh, and Linux file structures
- Identify the forensic tools used to identify the retrieve evidence from Windows, Macintosh, and Linux systems

# Introduction

- This chapter provides an overview of computer disk drives and how data is stored an managed on Microsoft, Macintosh, and Linux systems.
- It is essential that he computer forensic examiner understand the operation of these Oss to avoid damaging or destroying valuable evidence.
- Technical knowledge is required concerning the process of accessing and modifying system settings and options.
- A thorough understanding of disk drive operations, components, and configuration are required to successfully identify and retrieve digital data evidence.
- Forensic examination of disk drives and file system requires a considerable amount of education and practical experience.

# Disk Drive Overview

- The hard disk is the primary storage location where data is permanently stored. The four main components of a hard disk are:
  - Platters
  - Head arms
  - Chassis
  - Head actuator

- The capacity of a computer hard disk drive and the files it contains can be confusing.
- The capacity of the disk drive that is to be imaged will be concern to the forensic examiner.

**Table 9.1 Disk Capacity Values.**

| *Bit* | *Value of 0 or 1* |
|---|---|
| Nibble | 4 bits |
| Byte | 8 bits |
| Kilobit | 1,000 bits |
| Kilobyte | 1,000 bytes |
| Kibibit | 1,024 bits |
| Kibibyte | 1,024 bytes |
| Mebibit | 1,048,576 bits |
| Mebibyte | 1,048,576 bytes |
| Megabit | 1,000,000 bits |
| Megabyte | 1,000,000 bytes |
| Gibibit | 1,073,741,824 bits |
| Gibibyte | 1,073,741,824 bytes |
| Gigabit | 1,000,000,000 bits |
| Gigabyte | 1,000,000,000 bytes |
| Tebibit | 1,099,511,627,776 bits |
| Tebibyte | 1,099,511,627,776 bytes |
| Terabit | 1,000,000,000,000 bits |
| Terabyte | 1,000,000,000,000 bytes |

# Disk Drive Overview (Cont.)

- Most computer hard disk drives are permanently stored in an internal hard drive bay at the form of the compute and are connected with one ATA/SCSI cable and power cable.
- Disk drives are constructed of one or more cylinders (platters) coated with magnetic material.
- The geometry or configurations reflects the internal organization of the disk drive. The components that make up the physical disk patter includes :

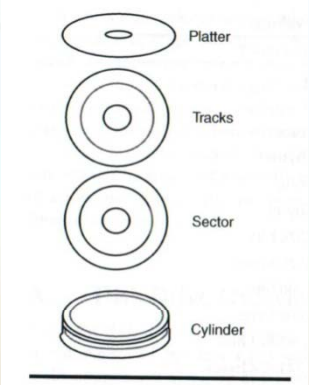

Figure 9.2 Disk drive geometry.

•A cylinder or platter: contains a set of tracks on a multiheaded disk that may be accessed without head movements.

•Tracks are addressable concentric rings on magnetic, secondary storage disks used for storing data.

•Sectors are the smallest using of storage on a disk.

- The boot sector is the very first sector on a hard drive.
- The master boot record (MBR) describes how the hard drive is organized.
- Digital images are written on the tracks as bytes.
- The typical hard disk has a storage capacity of 512 bytes per sector.

# Computer Hard Drive Interfaces

- Computer hard disk interfaces include various specifications of AT attachment drives.
- The computer interfaces allow a computer to send and retrieve information for storage devices, such as computer hard disk drives and CD-ROM drives.
- A brief description of these categories of drives will be useful to the forensic examiner.
  - ATA (AT Attachment) interfaces are the most commonly used interfaces on IBM-compatible computers.
  - ATAPI (AT Attachment Packet) is an extension to ATA that allow support for devices such as tape drives and other computer peripherals.
  - IDE (Integrated Drive Electronics) is more commonly knows as ATA and is a standard interface for IBM-compatible hard drives.
  - EIDE is the next generation of IDE interface that was developed by Western Digital and an interface commonly used on IBM compatible computers.
- CMOS or complementary metal oxide substrate uses logical block addressing and enhanced cylinder, head and sector configuration.

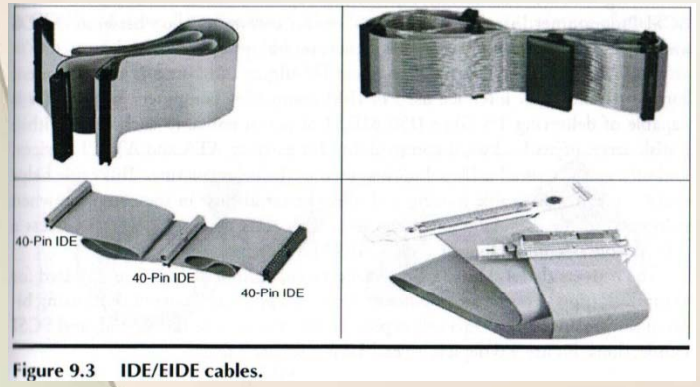

Figure 9.3 IDE/EIDE cables.

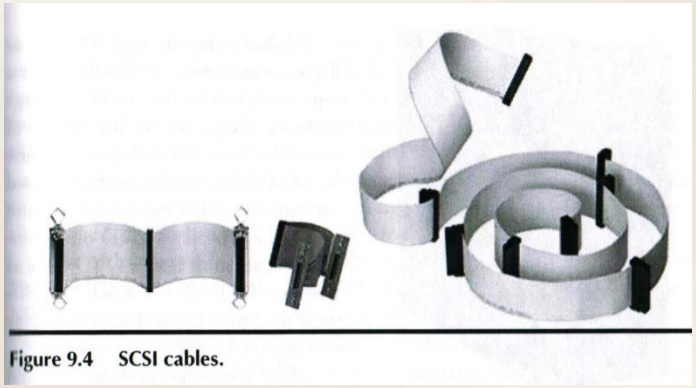
Figure 9.4 SCSI cables.

# Computer Hard Drive Interfaces (Cont.)

- Newer drives technology.
  - SCSI (Small Computer System Interface) is a standard for parallel interfaces that transfers information at a rate of 8 bps and fasters, which is faster than the average parallel interface.
  - SATA (Serial ATA) was first released in August 2001 and is a replacement for the parallel ATA interface use in IBM compatible computers.
  - USB (universal serial bus) is an external peripheral interface standard for communication between a computer and external peripherals over a cable using bi-serial transmission.

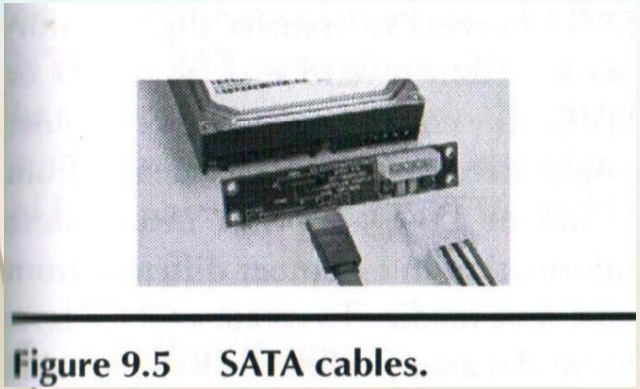

Figure 9.5 SATA cables.

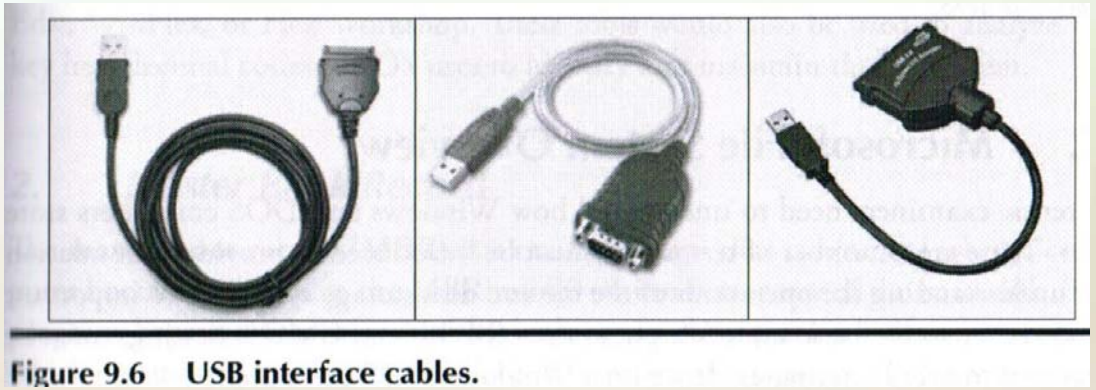

Figure 9.6 USB interface cables.

# Computer Hard Drive Interfaces (Cont.)

- Other technology.
  - RAID (Redundant array of Inexpensive disks) is an assortment of hard disk drives connected and setup in ways to help protect and/or speed up the performance of a computer's disk storage. RAID levels 1-5, 10, and 15 can be implemented through software or special hardware controllers.
  - CD (Compact Disk) is a flat round storage medium that is ready bay a laser in a CD-ROM drive.
  - DVD (Digital Versatile Disk) or DVD-ROM (Digital Video Disk) is a type of disk drive that allows for large amounts of data on one disk.
- Optical media store information in a manner different from magnetic media.
- On the surface of a CD, data is configured into three areas: lead-in, program, and lead-out.
- The computer forensics examiner might need to retrieve evidence from a DC or DVD.

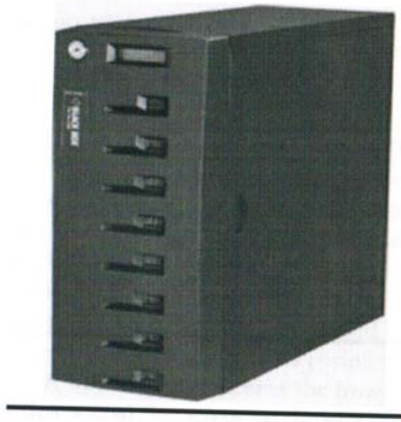

Figure 9.7 RAID storage device.

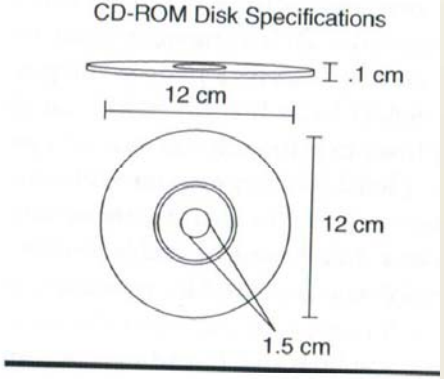


Figure 9.8 CD-ROM disk specifications.

# Microsoft File System Overview

- Forensic examiners need to understand how Windows and DOS computers store files.
- BIOS (Basic Input/output System) runs at the computer start-up where it configures devices and the boots the operating system.
  - BIOS information is stored on a ROM (Read-only Memory)
- Bootstrap is the first code executed when the computer is on.
- NTFS (New Technology File System) is Windows NT's replacement for the DOS FAT and OS/2's HPFS (High-performance File System
- FAT (File Allocation table) is a file system table used by the FAT-file system. It contains information about where on the disk the content of the files is stored.
  - There are three versions of FAT: FAT12, FAT 16, and FAT32

## Partitions

- A partition is a segment of the hard drive that is separated from other portions of the hard disk drive.
- It is possible for users to hide data in voids between partitions on hard drive. Theis unused space between partitions is called the partition gap.
- The forensic examiner can use a number of tools to examine a partition's physical level. This includes:
  - Norton Disk Edit,
  - WinHex
  - Hex Workshop

# Microsoft File System Overview (Cont.)

## Master Book Record

- MBR is a small program that is executed when a computer boots up.
- Typically, the MBR resides on the first sector of the hard disk.
- The MBR stores information about the partitions on a disk and their locations, size, and other critical items.

## Registry Data

- The registry consists of a database that contains hardware and software configuration, setup information and user preferences.
- The registry is used in Windows operating systems
- The forensic examiner might find useful information in the registry database.
- We have two versions Reedit and Regedit32
- The registry for Windows 9x is located in System.dat and User.dat, which is located in the Windows root directory.
- Registry information for Windows 2000 and XP is located in the Winnt\Config and Windows\System32\Regedt.exe.

## Windows Forensic Tools

- A number of computer forensic tools are describe on the vendors Webpage. Some include:
  - Trinity Rescue Kit (TRK), The Farmers' Boot CD, The SleuthKit, Autopsy Browser

# Macintosh Computer Systems

- The Macintosh (Mac) is an alternative PC platform to DOS-based PCs developed by Apple in the 1980s.
- The Map is a popular computer for schools and graphics professionals.
- The current Mac OS is Mac OS-X v.10.40.6
- Mac uses a HFS (Hierarchical File System) where files are stored in directories or folders.
- The file manager handles the reading, writing, and storage of data.
- The finder is another Mac tool that interacts with the OS to keep track of files and maintain each user's desktop
- The data fork contain data that the user creates.
  - Resource fork contains the menu, icons, dialog boxes, controls, and executable code.
- A volume is any storage media used to store files.
- An allocation block consist of the number of blocks assembled in the Mac file system when a file is saved.
  - A logical block is a collection not exceeding 512 bytes.
- The logical EOF refers to the number of bytes that contain data.
- The physical EOF represents the number of the allocation block for the file.
- Macintosh computers use open firmware instead of BIOS firmware.

# Macintosh Computer Systems (Cont.)

## Forensic Tools for Mac Systems

- Most forensic tool are oriented toward the Windows environment; however, new packages have become available to assist in investigation involving Mac computers.
  - MacForensicsLab
  - MacQuisition Boot CD
  - Open-Source forensics
  - Open-source forensic tools
- The Mac OS is a Unix-based system and most user files are created and saved in the user's home directory.

# UNIX/Linux Systems

- UNIX is an OS that originated at Bell labs in 1969 as an interactive time-sharing system
- UNIX became the first OS written in the C programming language.
- UNIX has evolved as a kind of large freeware product with a variety of versions
- UNIX is well-known for its relative hardware independence and portable application interfaces.
- Linux is a version of UNIX that urns on a variety of hardware platforms.
- Linux uses inodes, or information nodes , that contain deceptive information about each file or directory.
  - The inode number is an integer unique to the device upon which it is stored.
  - All files are hard links to inodes.
  - An inode is a pointer to other inodes or blocks.
  - Each inode keeps an internal link count, and when the number becomes 0, Linux deletes the file.
- Everything is UNIX and Linux is a file.
- All UNIX files are defined as objects,.
- UNIX consist of boot block, superblock, inode and data block components that define the file system.
  - A block is a disk allocation unit that ranges from 512 bytes and up.
- A partition is a logical section of a disk.

# UNIX/Linux Systems (Cont.)

## Examining a UNIX or Linux System

- The forensic personnel must first review the documentation of the UNIX system being examined for information concerning the boot process and other specifics to a particular system.
- UNIX system, such as file servers or Web servers, probably cannot be powered down.
- There are also specific processes that occur when powering on a UNIX workstation.

## UNIX and Linux Forensic Tools

- UNIX and Linux tools are available from a number of sources including:
  - SMART Linux: Is a live DC and an installable distribution of Linux designed for DATA Forensics and Incident Response from ASR Data
  - ForensiX, Linux Forensic eXaminer: Collects and analyzes digital evidence.
  - Maresware: Catalog, hashes and strings searching programs