Certified Hacking Forensics Investigator

Module #03 : Understanding Hard Disks and File Systems

Eng. Mohammad Khreesha
Twitter: @banyrock
Facebook : http://www.fb.com/khreesha

Module Objectives

➔ **After Successfully completing this module, you will be able to :**

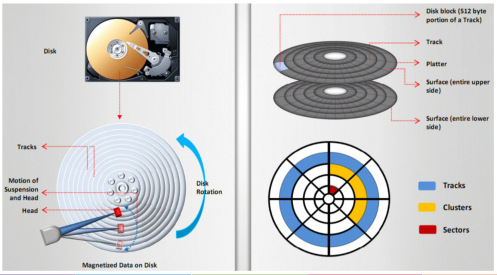
1. Describe the different types of disk drives and their characteristics.
2. Understand the physical and logical structure of a hard disk.
3. Identify the types of hard disk interfaces and discuss the various hard disk components.
4. Describe hard disk partitions.
5. Summarize Windows, Max, and Linux boot Processes.
6. Understand various Windows, Linux, and Mac OS X file systems.
7. Differentiate between various RAID storage systems.
8. Demonstrate file system analysis.

Disk Drive Overview

➔ **Hard Disk Drive (HDD)**
- The HDD is non-volatile, random access digital storage device used in any computer system.
- It utilizes a mechanism that reads data from a disk and writes onto an another disk.
- The hard disk record data magnetically.

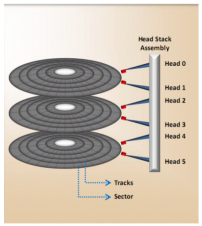
➔ **Solid-state Drive (SSD)**
- The SSD is a data storage device that uses solid-state memory to store data and provides access to the stored data in the same manner as a HDD.
- It uses microchips to hold data in non-volatile memory chips and does not contain any moving parts.
- It is very expensive per gigabyte and supports a restricted number of writes over the life of the device.
- It uses two memories:
  - NAND-based flash memory: It retains memory even without power.
  - Volatile RAM: It provides faster access.

Physical Structure of Hard Disk



Tracks

- Tracks are the concentric circles on platters where all the information is stored.
- Drive head ca access these circular rings in one position at a time.
- Tracks are numbers for identification purposes.
- Read-write is done by rolling headers from inner to outermost part of the disk.



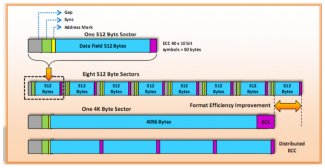
Sector

- A sector is the smallest physical storage unit on the disk platter.
- It is almost always 512 bytes in size and a few additional bytes for drive control and error correction.
- Each disk sector is labeled using the factory track-positioning data.
- The optimal method of storing a file on a disk is in a contiguous series.
- For example, if the file size is 600 bytes, two 512 bytes sectors are allocated for the file.

- **Sector Addressing:**
  - Cylinders, heads and sectors determine the address of the individual sectors on the disk.
  - For example, on formatting a disk, 50 tracks are divided into 10 sectors each.
  - Track and sector numbers are used by the operating system and disk drive to identify the stored information.

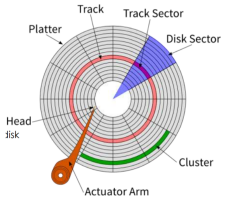
Advanced Format : Sector

- New hard drives use 4096 bytes advanced format sectors.
- Generation-one Advanced Format also called as 4K sector technology, efficiently uses the storage surface media of a disk efficiently by merging eight 512 byes sectors into one single sector.
- After merging, the structure of 4K sector does not disturb the key design elements of the traditional 512 bytes sector.



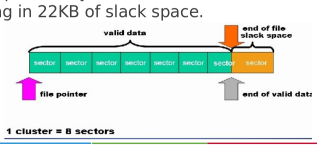
Clusters

A cluster is the smallest logical storage unit on a hard disk. It is a set of track sectors, ranging from 2 to 32 or more, depending on the formatting scheme in use.



Slack Space

- Slack space is the area of a disk cluster between the end of the file and the end of the cluster.
- If the file size is less than the cluster size, still a full cluster is assigned to that file. The remaining space remains unused and is called slack space. This remaining unused space is called slack space.
- For example, if the partition size is 4GB, each cluster will be 32KB. Even if a file requires only 10KB, the entire 32KB will be allocated to that file, resulting in 22KB of slack space.



Lost Clusters

- When the operating system marks clusters, as used, but does not allocate them to any file, such clusters are known as lost clusters.
- A lost cluster is a FAT file system error that results from in what manner the FAT file system allocates space and chains files together.
- It is mainly the result of a logical structure error and not physical disk error.
- They usually occur because of interrupted file activities such as, 'the file is not correctly completed and closed' thus, the clusters have involved never linked correctly to a file.
- CHKDSK is a system tool in Windows, that authenticates the file system reliability of a volume and repairs logical file system errors.

Bad Sectors

- Bad sector is a damaged portion of a disk on which no read/write operation can be performed.
- Formatting a disk enables the OS to identify unusable sectors and mark them as bad sectors.
- Bad sectors are formed due to configuration problems or any physical disturbances to the disk.
- If data is in a sector that becomes bad, then it might not be recoverable. Data can be recovered using software tools such as CHKDSK.

Disk Capacity Calculation

- A disk drive has 16,384 cylinders, 80 heads, and 63 sectors/track. Assume, a sector has 512 bytes. What is the capacity of such a disk?

Answer :

1 disk

16,384 cylinders/disk

80 heads/cylinder

1 track/head

63 sectors/track

512 bytes/sector

Total disk size (in bytes) = 1 disk * (16,384 cylinders/disk) * (80 heads/cylinder) * (1 track/head) * (63 sectors/track) * (512 bytes/sector) = 42,278,584,320 bytes

Disk Partitions

- The HDD partitioning is the creation of logical divisions upon a hard disk that allows user to apply operating system-specific logical formatting.
- **Primary Partition**: It is a drive that holds the information regarding OS, system area, and other information required for booting (C: partition in windows).
- **Extended Partition**: It is the logical drive that holds information regarding stored data and files in the disk.

Continue

BIOS Parameter Block

- The BIOS parameter block (BPB) is a data structure in the partition boot sector.
- It describes the physical layout of data storage volume, like the number of heads and the size of the tracks on the drive.
- BPB assists investigators to locate the file table on the HDD.

Master Boot Record

- Master boot record (MBR) us the first sector of a data storage device, such as a HDD.
- The information regarding the files on the disk, their location, size, and other important data is stored in the MBR file.
- In practice, MBR is almost always refers to the 512-byte boot sector or partition sector of a disk.
- In UNIX/Linux, dd command can e used to backup and restore the MBR:
  - Backup:
    - dd if=/dev/xxx of=mbr.backup bs=512 count=1
  - Restore:
    - dd if=mbr.backup of=/dev/xxx bs=512 count=1

Globally Unique Identifiers (GUID)

- Global Unique Identifier (GUID) is a 128-bit unique reference number used as an identifier in computer software.
- In general, GUIDs are displayed as 32 hexadecimal digits with group separated by hyphens.
- Common Uses:
  - In Windows registry, they are used to identify COM DLLs.
  - In database tables, they are used as primary key values.
  - Website assigns GUID to a user's bowser to record and track the session.
  - Windows assigns GUID to a username to identify user accounts.

GUID Partition Table (GPT)

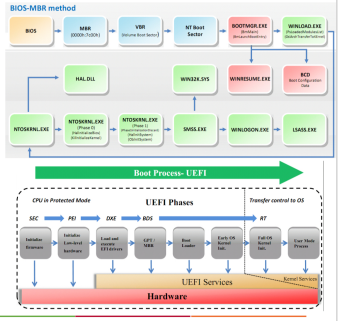
- UEFI replaces legacy BIOS firmware interfaces.
- UEFI is a specification that defines a software interface between an OS and platform firmware.
- It uses a partition system known as GUID Partition Table (GPT) that replaces the traditional MBR.
- **Advantages of GPT disk layout:**
  - Supports up to 128 partitions ans uses 64-bit Logical Block Addresses.
  - Supports maximum partition size from 2 TiB to 8 ZiB.
  - Provides primary and backup partition tables for redundancy

Booting Process

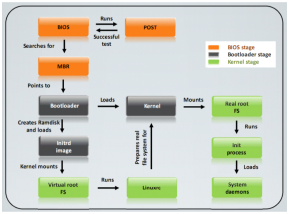
- Booting refers to the process of starting or resetting OS when user turns on a computer system.
- It loads the OS which is stored in the disk to the RAM.
- Types of Booting:
  - **Cold boot (Hard boot):**
    - It is the process of starting a computer from a powered-down or off state.
  - **Warm boot (Soft boot):**
    - It is the process of restarting a computer that is already turned on through the OS.

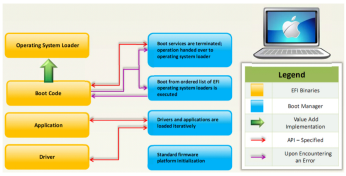
Windows Booting Process

File Names	Description
Ntoskrnl.exe	Executive and kernel
Ntkrnlpa.exe	Executive and kernel with support for Physical Address Extension (PAE)
Hal.dll	Hardware abstraction layer
Win32k.sys	Kernel-mode part of the Win32 subsystem
Ntdll.dll	Internal support functions and system service dispatch stubs to executive functions
Kernel32.dll	Win32 subsystem DLL files
Advapi32.dll	
User32.dll	
Gdi32.dll	



Linux/Mac OS X Boot Process





File Systems

- The file system is a set of data types, which is employed for storage, hierarchical categorization, management, navigation, access, and recovering the data.
- It provides a mechanism for users to store data logically in a hierarchy of files and directories.
- It also includes a format for specifying the path to a file through the structure of directories.
- They are organized in the form of tree-structured directories, and directories require access authorization.
- Major file systems include : FAT, NTFS, HFS, HFS+, Ext2, Ext3, EXt4, ... etc.
- **Types of File Systems:**
  - Shared Disk File Systems
  - Disk File Systems
  - Special Purpose File Systems
  - Network File Systems
  - Tape File Systems
  - Database File Systems
  - Flash File Systems

Windows File Systems

Fat (File Allocation Table)

File Allocation Table is a method of organization of internal data that resides at the beginning of the volume
It is a 16-bit Ale system and was developed for DOS and further supported by all operating systems

FAT32

- It is a 32-Nt version of FAT file system using smaller clusters and result in efficient storage capacity
- It supports drive size up to 2 terabytes

NTFS (New Technology File System)

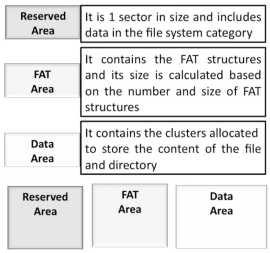
- NTFS provides for enhanced security file-by-file compression, quotas, and even encryption
- It is developed to rapidly carry out standard file operations such as read, write, search file system recovery

File Allocation Table (FAT)

- Fat (File Allocation Table) file system designed in 1976
- It is the main file system for many operating systems such as DOS, Window open DOS etc.
- File allocation table stores all the files and resides at the beginning of the volume
- FAT contains three different versions (FAT12, FAT16, and FAT32) and differs due to the size of the entries r1 the FAT structure

System	Bytes Per Cluster within File Allocation Table	Cluster Limit
FAT12	1.5	Fewer than 4087 clusters
FAT13	2	Between 4,087 and 65,526 clusters, inclusive
FAT32	4	Between 65,526 and 268, 435, 456, clusters, included

FAT File System Layout



Root Directory

File Name	Size	Cluster
Gary.txt	1034	6
Hello.jpg	3973	3

File Allocation Table

Cluster	Next
2	0
3	8
4	0
5	0
6	0xFF
7	0
8	0xFF
9	0

FAT32 File System

- FAT32 file system is derived from a FAT file system and supports drives up to 2TB in size.
- It uses drive space efficiently and uses small clusters.
- t takes backup of the file allocation table instead of the default copy.

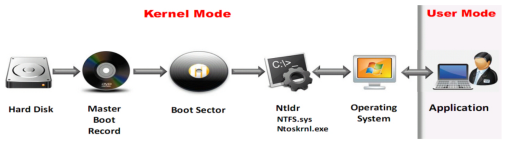
Offset	Description	Size
000h	Executable Code (Boots Computer)	446 Bytes
1BEh	1st Position Entry	16 Bytes
1CEh	2nd Position Entry	16 Bytes
1DEh	3rd Position Entry	16 Bytes
1EEh	4th Position Entry	16 Bytes
1FEh	Boot Record Signature	2 Bytes

MBR table of FAT32

NTFS File System

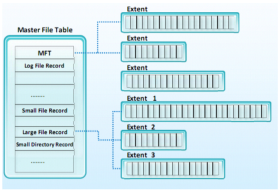
Volume Size	Sectors Per Cluster	Default Cluster Size
512 MB or less	1	512 bytes
513 MB – 1024 MB (1 GB)	2	1024 bytes (1 GB)
1024 – 2048 MB (2 GB)	4	2048 bytes (2 GB)
Greater than 2049 MB	8	4 KB

File Name	Description
$attrdef	Contains definitions of all system-and user-defined attributes of the volume
$badclus	Contains all the bad clusters
$bitmap	Contains bitmap for the entire volume
$boot	Contains the volume's bootstrap
$logfile	Used for recovery purposes
$mft	Contains a record for every file
$mftmirr	Mirror of the MFT used for recovering files
$quota	Indicates disk quota for each user
$upcase	Converts characters into uppercase Unicode
$volume	Contains volume name and version number



NTFS Master File Table (MFT)

- MFT is a relational DB, which consists of information related to the files and the file attributes.
- The rows consist of file records and the columns consist if file attributes.
- It has information of every file on the NTFS volume including its own information.
- It has 16 records reserved for system files.



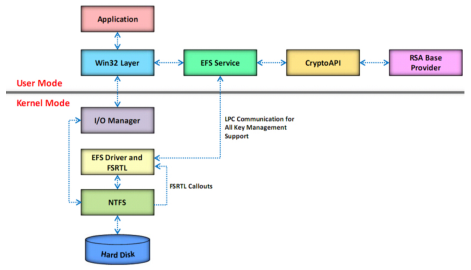
System File	File Name	MFT Record	Purpose of the File
Master file table	$Mft	0	It contains one base file record for each file and folder on an NTFS volume
Master file table mirror	$MftMirr	1	It guarantees access to the MFT in case of a single-sector failure
Log file	$LogFile	2	It contains information used by NTFS for faster recoverability
Volume	$Volume	3	It contains information about the volume
Attribute definitions	$AttrDef	4	It lists attribute names, numbers, and descriptions
Root file name index		5	The root folder
Cluster bitmap	$Bitmap	6	It represents the volume by showing free and unused clusters
Boot sector	$Boot	7	It includes the BPB used to mount the volume
Bad cluster file	$BadClus	8	It contains bad clusters for a volume
Security file	$Secure	9	It contains unique security descriptors for all files within a volume
Upcase table	$Upcase	10	It converts lowercase characters to matching Unicode uppercase characters
NTFS extension file	$Extend	11	It is used for various optional extensions

NTFS Data Stream

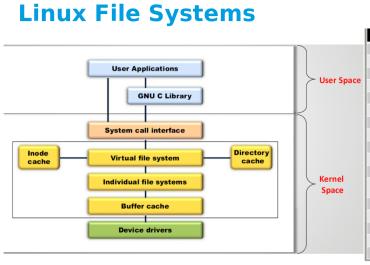
- NTFS data stream is a unique set of file attributes.
- NTFS supports multiple data streams per file, where the stream name identifies a new data attribute on the file.
- Example :
  - echo <text data> > file.txt:stream_data

Attribute Type	Purpose of the Attribute
Standard information	Lists the information regarding the time stamp data and link count information
Attribute list	List of attributes that are not in the MFT
File name	The file name is stored here and can be a long or short name
Security descriptor	Ownership and access rights to the file are listed here
Data	Stores file data
Object id	File identifier volume –unique identifier
Logged tool stream	Used by the encrypted file system service
Reparse point	Volume mount point used for installable file system filter drivers
Index root	Employed for use of folders and files
Index allocation	Employed for use of folders and files
Bitmap	Employed for use of folders and files
Volume information	Version number of the volume is listed
Volume name	The volume label is listed here

Encrypting File System (EFS)



Linux File Systems



Directory	Description
/bin	Essential command binaries. Ex: cat, ls, cp.
/boot	Static files of the boot loader. Ex: Kernels, Initrd
/dev	Essential device files. Ex: /dev/null
/etc	Host-specific system configuration files
/home	Users' home directories, holding saved files, personal settings, etc.
/lib	Essential libraries for the binaries in /bin/ and /sbin/
/media	Mount points for removable media
/mnt	Temporarily mounted filesystems
/opt	Add-on application software packages
/root	Home directory for the root user
/proc	Virtual file system providing process and kernel information as files
/run	Information about running processes. Ex: running daemons, currently logged-in users
/sbin	Contains the binary files required for working
/srv	Site-specific data for services provided by the system
/tmp	Temporary files
/usr	Secondary hierarchy for read-only user data
/var	Variable data. Ex: logs, spool files, etc.

Continue..

EXT
(Extended File System)
- First file system for the Linux operating system to overcome certain limitations of the Mmix file system
- It is replaced by the second extended file system

EXT2
(Second Extended File System)
- 9 Standard file system with improved algorithms used on the Linux operating system for a number of years
- 9 Not a journaling file system

EXT 3 -(Third Extended File System)
- Journaled file system used in the GNU/Linux operating system
- It is mounted and used as an Ext2 file system
- It uses file system maintenance utilities (like fsck) for maintaining and repairing alike Ext2 file system

MAC OS X File Systems

HFS (Hierarchical File System)

Developed by Apple Computer to support Mac operating system

HFS Plus

HFS Plus CHFS+) is a successor of HFS and is used as a primary file system in Macintosh

UFS (UNIX File System)

- Derived from the Berkeley Fast File System (FFS that was originally developed at Bell Laboratories from the first version of UNIX FS
- All BSD UNIX derivatives including FreeBSD, NetBSD, OpenBSD, NeXTStep, and Solaris use a variant of UFS
- Acts as a substitute for HFS in Mac OS X

RAID Storage System

- Redundant Array of inexpensive Disks (RAID) is a technology that uses multiple smaller disks simultaneously which function as a single large volume
- It provides a particular method of accessing one or many separate hard disks, thereby decreasing the risk of losing all data if any one hard disk fails or is damaged, and improving access time
- This technology is developed to:
  - Maintain a large amount of data storage
  - Achieve a greater level of input/output performance
  - Achieve a greater reliability through data redundancy

RAID Level 0 (Disk Stripping)

- Data is split into blocks and written equally across multiple hard drives
- It improves I/O performance by spreading the 110 load across many channels and disk drives
- If any drive fails, data recovery is not possible
- It does not provide data redundancy
- It requires minimum two drives for set up

RAID Level 1 (Disk Mirroring)

- Multiple copies of data are written to multiple drives at the same time
- It provides data redundancy by completely duplicating the drive data to multiple drives
- If one drive fails, data recovery is possible
- It requires minimum two drives for set up

RAID Level 3 (Disk Stripping with Parity)

- Data is striped at a byte level across multiple drives and one drive is set to store parity information
- If any drive fails, data recovery and error correction is possible through the parity drive
- Parity drive stores all the information about the data on multiple drives

RAID Level 5 (Block Interleaved Distributed Parity)

- Data is striped at a byte level across multiple drives and parity information is distributed among all member drives
- Data writing process is slow
- It requires a minimum of three drives for setup

RAID Level 10 (Blocks Stripped and Mirrored)

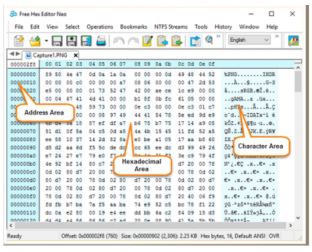
- RAID 10 is a combination of RAID 0 (Striping Volume Data and RAID 1 (Disk Mirroring) and requires at least four drives to implement
- It has same fault tolerance as RAID level 1 and the same overheads as mirroring alone
- It allows mirroring of disks in pairs for redundancy and improved performance, and then data is striped across multiple disks for maximum performance

File Systems Analysis

- American Standard Code for Information Interchange (ASCII)
  - 128 specified characters coded into 7-bit integers.
  - Source code of a program, batch files, macros, scripts, HTML and XML documents
  - 0 to 9, a-z, A-Z, Basic punctuation symbols, Control codes that originated with teletype machines
  - ASCII table has 3 divisions namely, non-printable (system codes between 0 and 31), lower ASCII (codes between 32 and 127), and higher ASCII (codes between 128 and 255). The graphics files and documents use non-ASCII characters made in word processers, spreadsheet or database programs and sent as email

- Unicode computing standard developed with the Universal Coded Character Set (UCS)
  - Standard for encoding, representation, and management of texts, which most of the world's writing systems use.
  - More than 128,000 characters from about 135 modern and historic scripts
  - Technologies such as modern operating systems, XML, Java, and the Microsoft .NET Framework have adopted the Unicode standards.

Continue..

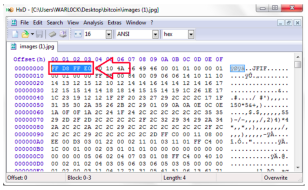


HEX	Binary	Base 10
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
A	1010	10
B	1011	11
C	1100	12
D	1101	13
E	1110	14
F	1111	15

File Carving

- It is a technique to recover files and fragments of files from unallocated space of the disk in the absence of the file metadata.
- In this technique, file identification and extraction is based on certain characteristics like file header or footer rather than the file extension or metadata.

TERM	DEFINITION
Block	The size of the smallest data unit that can be written to storage media. It refers to either the sector or the cluster size.
Header	Header blocks contain the starting point of a file.
Footer	Footers contain the ending point of a file.
Fragment	One block or a sequence of blocks that belong to one file.One file can be built from different fragments which are not sequentially connected to each other. The distance between different fragments of one file is unknown, further it is possible that fragments do not exist anymore becausethey have been overwritten.
Base-fragment	The first fragment of a file. It contains the header (if available for the filetype investigated).
Fragmentation point	The last block of a file before fragmentation occurs. As a file can consist of multiple fragments it is possible that there exist multiple fragmentation points.
Fragmentation area	Consecutive blocks which are grouped into a set and which contain the fragmentation point.



Follow us :

- https://www.fb.com/technawidotcom
- https://www.twitter.com/technawidotnet
- http://www.technawi.net