

**Prifysgol Cymru**  
Y Drindod Dewi Sant  
**University of Wales**  
Trinity Saint David

**200**  
**1822 - 2022**

*Man Geni Addysg Uwch yng Nghymru*  
*Where Higher Education Began in Wales*



Prifysgol Cymru  
Y Drindod Dewi Sant  
University of Wales  
Trinity Saint David

200  
1822 - 2022

# Digital Forensics: Analysing Evidences

*Digital Forensics*  
(ACCA7031)

Applied Computing - WISA

*Man Geni Addysg Uwch yng Nghymru*  
*Where Higher Education Began in Wales*

[www.uwtsd.ac.uk](http://www.uwtsd.ac.uk)



## ➤ **Analysing Evidences**

- **Disk**
- **Partitions**
- **File System**
- **Attributes**

## **Lab/ Tutorials**

### ➤ **Handson Activity 3**

*Man Geni Addysg Uwch yng Nghymru  
Where Higher Education Began in Wales*

*In continuation to our earlier lecture, we discussed about the History of Digital Forensics and its attributes. Understood the importance of Incident Response and discussed about the principles of Digital Forensics, its process, different roles and finally getting to understand the technology's role in the crime and the law framed around it to prevent various crimes.*

*Today, during the lecture, lets move forward and discuss about various digital forensics capabilities and the appropriate method to acquire data. We shall also discuss the challenges in acquiring data and the area in which keen attention is required. Our discussion this week will cover digital evidences storage formats, Acquisition Methods, Contingency Planning for Data Acquisition, Use and Validate Data Acquisition, RAID Acquisition, Remote Network Acquisition and Forensic Tools used for Data Acquisition.*

# Understanding the silent witness!!!

- Gives OS a road map to data on a disk
- Type of file system determines how data is stored on the disk
- A file system is directly related to an OS
- On investigating a suspect's computer to acquire or inspect data, You should be familiar with the computer's platform



Storage Drives and its characteristics



Logical Structure of a Disk



Booting Process



File Systems and Storage Systems



Prifysgol Cymru  
Y Drindod Dewi Sant  
University of Wales  
Trinity Saint David

200  
1822 - 2022

Man Geni Addysg Uwch yng Nghymru  
Where Higher Education Began in Wales

## Discussion Point

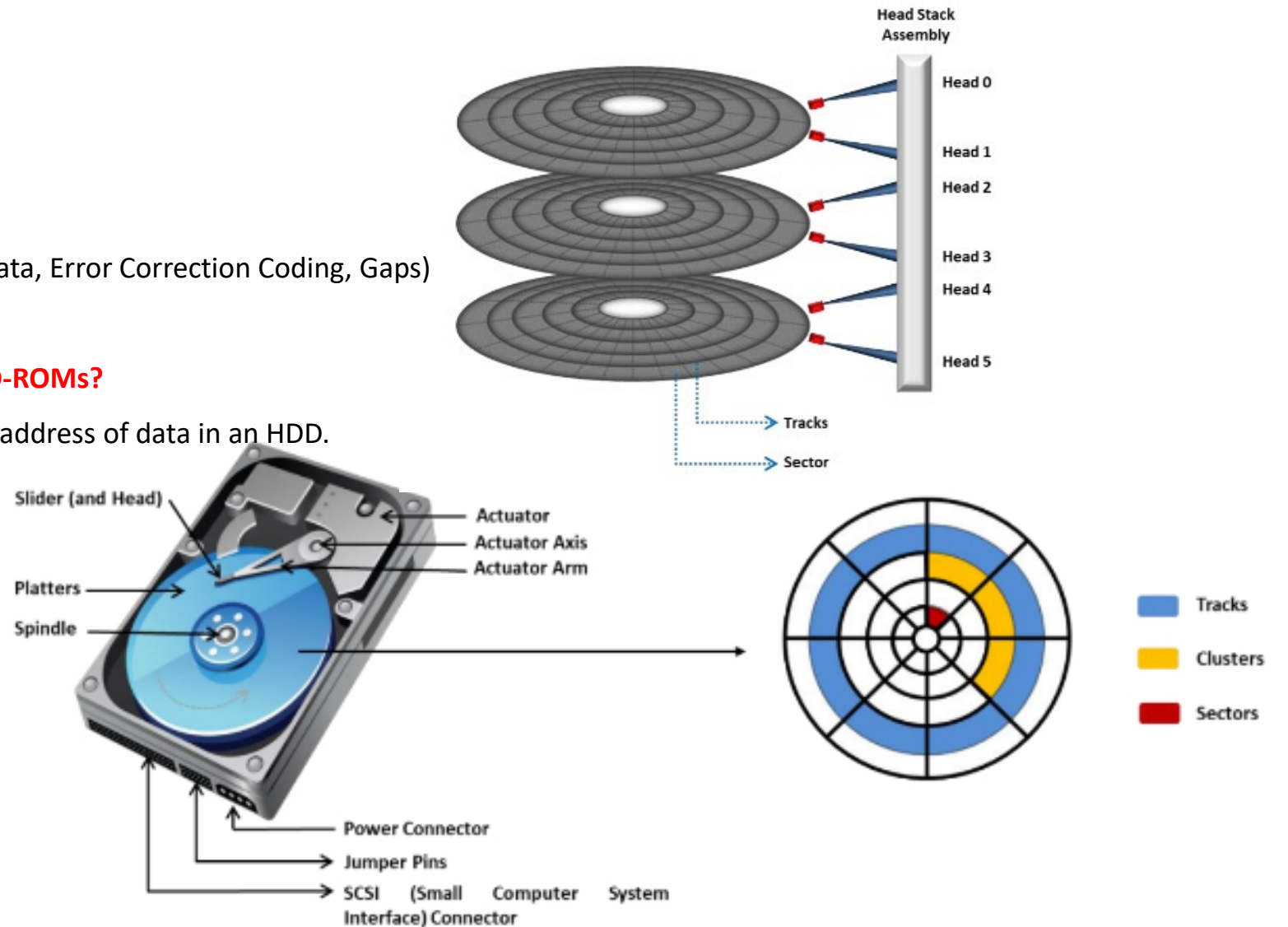
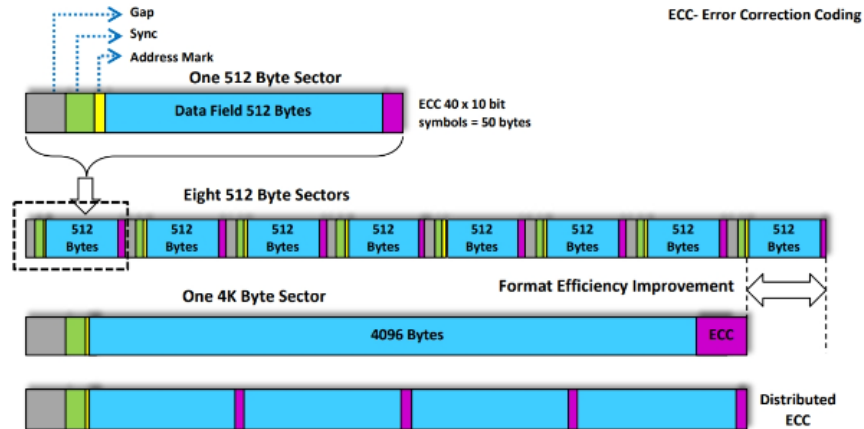
- Understand file systems and its unique characteristics – for digital forensics
- HDD vs SSD
  - Data is the Key – a silent witness – Unlock and interpret this silence
  - File systems are blueprints
  - Storage drives are digital evidences
  - Knowing the ins and outs of file system, its characteristics help in extracting and analysing the data
  - Working on this area will help you uncover challenges and opportunities
- HDD File Structure and Characteristics
- SSD File Structure and Characteristics
- File Systems in Digital Forensics



# Storage Disks

## ○ HDD

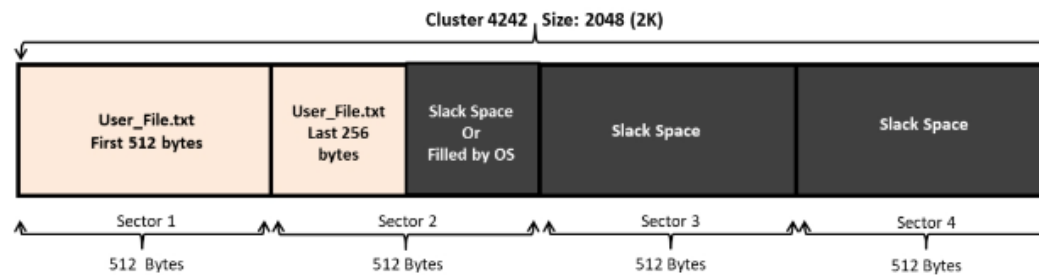
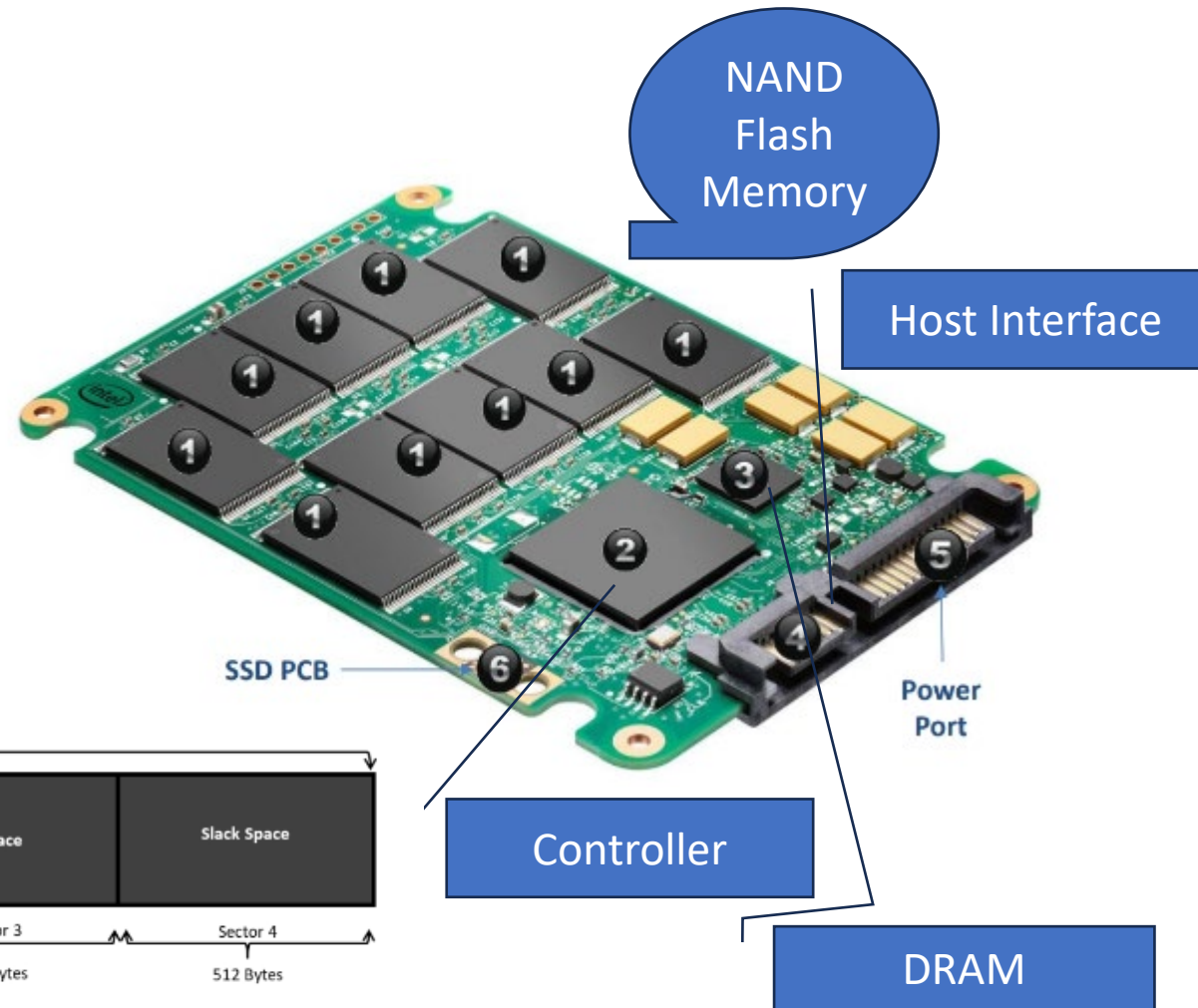
- Track Numbering
- Sector (ID Information, Synchronization Fields, Data, Error Correction Coding, Gaps)
- The data is stored is placed in a 512 bytes.
- **What is the bytes of data for CD-ROMs and DVD-ROMs?**
- The track number and sector number points the address of data in an HDD.
- **What is 4K Sectors?**



The images in this slide are used from Computer Hacking Forensic Investigator V10 eBook

# Storage Disks

- SSD
  - NAND-based SSDs
  - Volatile RAM-based SSDs
  - Advantages: Faster data access, lower power usage, High
- Data Addressing
  - Allotting addresses to each physical block of data
  - CHS (Cylinder-Head-Sector)
  - LBA (Logical Block Address)



## ○ What is Slack Space?

- RAM Slack and Drive Slack

The images in this slide are used from Computer Hacking Forensic Investigator V10 eBook

# Logical View

```
C:\Windows\system32>chkdsk
The type of the file system is NTFS.
Volume label is Local Disk.

WARNING! /F parameter not specified.
Running CHKDSK in read-only mode.

Stage 1: Examining basic file system structure ...
 830464 file records processed.
File verification completed.
Phase duration (File record verification): 17.41 seconds.
 14047 large file records processed.
Phase duration (Orphan file record recovery): 0.00 milliseconds.
 0 bad file records processed.
Phase duration (Bad file record checking): 0.26 milliseconds.

Stage 2: Examining file name linkage ...
 68622 reparse records processed.
 1198424 index entries processed.
Index verification completed.
Phase duration (Index verification): 25.71 seconds.
 0 unindexed files scanned.
Phase duration (Orphan reconnection): 8.98 seconds.
 0 unindexed files recovered to lost and found.
Phase duration (Orphan recovery to lost and found): 0.30 milliseconds.
 68622 reparse records processed.
Phase duration (Reparse point and Object ID verification): 163.55 milliseconds.

Stage 3: Examining security descriptors ...
Security descriptor verification completed.
Phase duration (Security descriptor verification): 39.63 milliseconds.
 183981 data files processed.
Phase duration (Data attribute verification): 0.37 milliseconds.
CHKDSK is verifying Usn Journal...
 35299040 USN bytes processed.
Usn Journal verification completed.
Phase duration (USN journal verification): 218.86 milliseconds.

Windows has scanned the file system and found no problems.
No further action is required.

248730623 KB total disk space.
240123288 KB in 631396 files.
 478400 KB in 183982 indexes.
 0 KB in bad sectors.
 995623 KB in use by the system.
 65536 KB occupied by the log file.
 7133312 KB available on disk.

    4096 bytes in each allocation unit.
 62182655 total allocation units on disk.
 1783328 allocation units available on disk.
Total duration: 52.55 seconds (52558 ms).

C:\Windows\system32>
```

- The logical view of the storage!!! – The File System
- File system is a controller of the physical disks (storage)
- File system is structured to focus on Performance, Consistency, Expandability and Compatibility of the physical disks
- **What happens when a cluster is marked as used but not allocated to any file?**
- **Lost Clusters**
  - What is the reason for Lost Clusters?
  - Does your storage have lost clusters? Find out.
- **“Bad Sectors” – What happens to a data in the bad sector? Could it be recovered?**



# Disk Partitions

## BIOS Parameter Block

- It is a data structure in the partition boot sector
- Defines the Filesystem Structure
- Assist investigations by locating the file table on the hard drive

## Master Boot Record

- First sector of a data storage device (HDD)
- The information about the files on the disk is stored in the MBR
- 512 Byte Boot Sector

**Let's look and analyse a MBR Structure: In Class Activity – Refer to our lecture demonstration about analysing MBR**

# MBR

To recall, the MBR holds 512 bytes (1 sector)– containing bootstrapping code, details of hard disk partition scheme etc. We just discussed and analysed about Sector 0, that has boot indicator, CHS Values, Partition Type, Size etc. Using MBR, what could be the maximum size of a Hard Disk?

A 512 GB

B 500 GB

C 1 TB

D 2 TB

Why?

446 CODE AREA

16 Bytes/row  
2 Hexa - 1 Byte

| Offset (d)   | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | Decoded text |
|--------------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|--------------|
| 000000000000 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....        |
| 000000000016 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....        |
| 000000000032 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....        |
| 000000000048 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....        |
| 000000000064 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....        |
| 000000000080 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....        |
| 000000000096 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....        |
| 000000000112 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....        |
| 000000000128 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....        |
| 000000000144 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....        |
| 000000000160 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....        |
| 000000000176 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....        |
| 000000000192 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....        |
| 000000000208 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....        |
| 000000000224 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....        |
| 000000000240 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....        |
| 000000000256 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....        |
| 000000000272 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....        |
| 000000000288 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....        |
| 000000000304 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....        |
| 000000000320 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....        |
| 000000000336 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....        |
| 000000000352 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....        |
| 000000000368 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....        |
| 000000000384 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....        |
| 000000000400 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....        |
| 000000000416 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....        |
| 000000000432 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....        |
| 000000000448 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....        |
| 000000000464 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....        |
| 000000000480 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....        |
| 000000000496 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....        |
| 000000000512 | 45 | 16 | 19 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....        |
| 000000000528 | 80 | E5 | 81 | A5 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....        |
| 000000000544 | AF | 32 | CF | 1D | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....        |
| 000000000560 | 5E | 32 | CF | 1D | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....        |
| 000000000576 | A1 | EF | B1 | FA | C8 | C8 | F2 | F5 | 02 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....        |

64 MASTER PARTITION TABLE

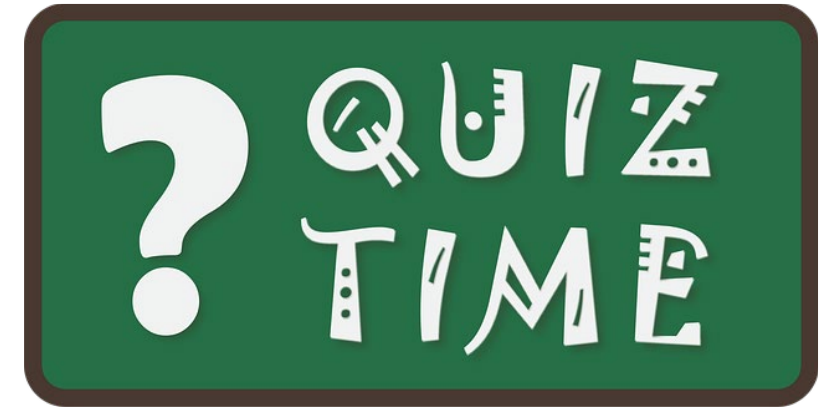
END OF MBR

BOOT RECORD SIGNATURE

Sample MBR in a Hexadecimal display

4 Partition  
16 Bytes each

1st-Byte - Boot Indicator  
NEXT 3 -Byte - Start of CHS values  
CYLINDER - HEAD - SECTOR  
NEXT 1 -Byte - Partition Type Descriptor  
NEXT 3 -Byte - END CHS VALUE  
NEXT 4 -Byte - STARTING SECTOR  
NEXT 4 -Byte - PARTITIONS SIZE



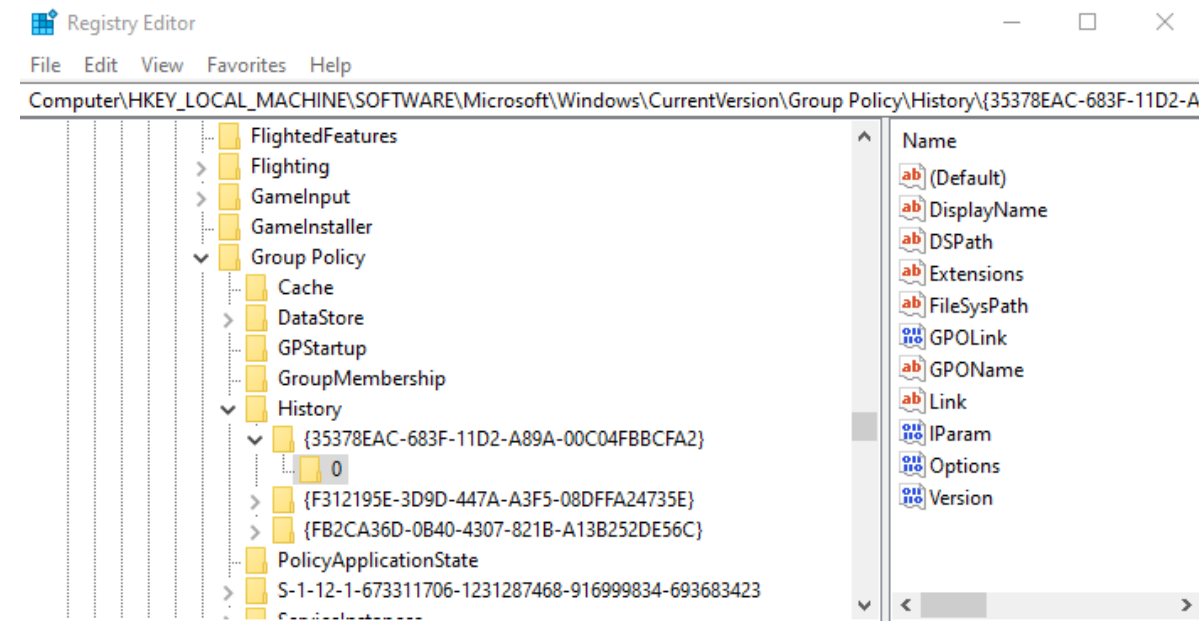
# Disk Partitions

## Globally Unique Identifier (GUID)

- 128-bit **unique** number generated by the Windows OS
- 32 Hexadecimal digits
- Identify a specific device, a document, a database entry, and/or user

## Globally Unique Identifier (GUID) Partition Table

- Modern and Standardized Partitioning Scheme.
- Replacement for MBR
- Part of UEFI
- MBR uses \_\_\_\_\_ bits for storing LBAs and the Size information on \_\_\_\_\_ byte sectors.
- GPT uses LBA instead of CHS
- Each block is 512 bytes, and each partition entry is 128 bytes.



**Let's look and analyse a GPT Structure: In Class Activity – Refer to our lecture demonstration about analysing GPT**

# Disk Partitions

## Globally Unique Identifier (GUID) Partition Table

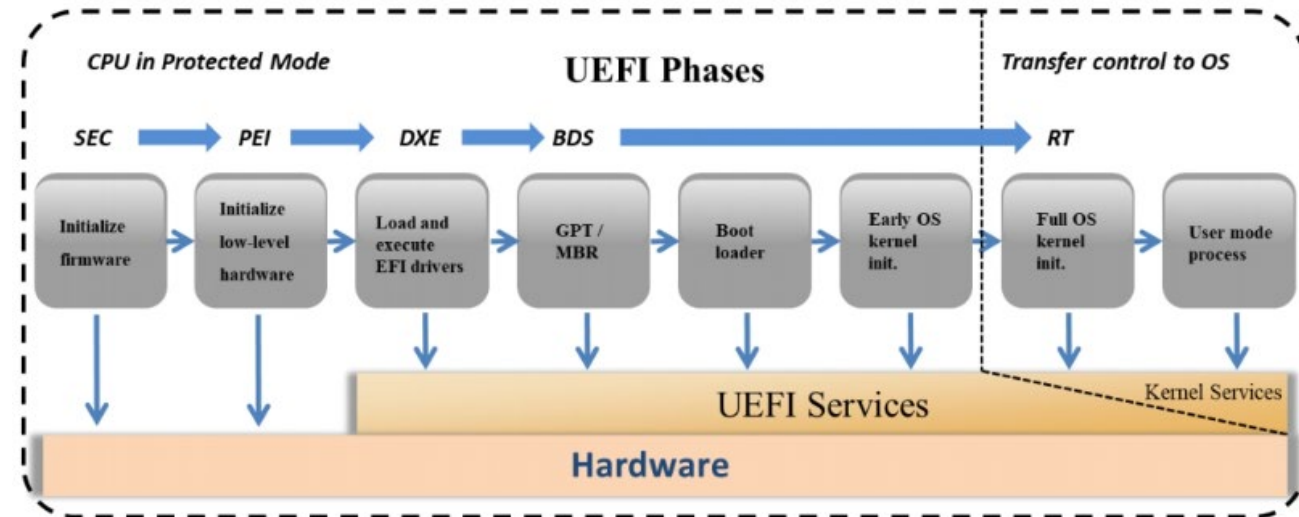
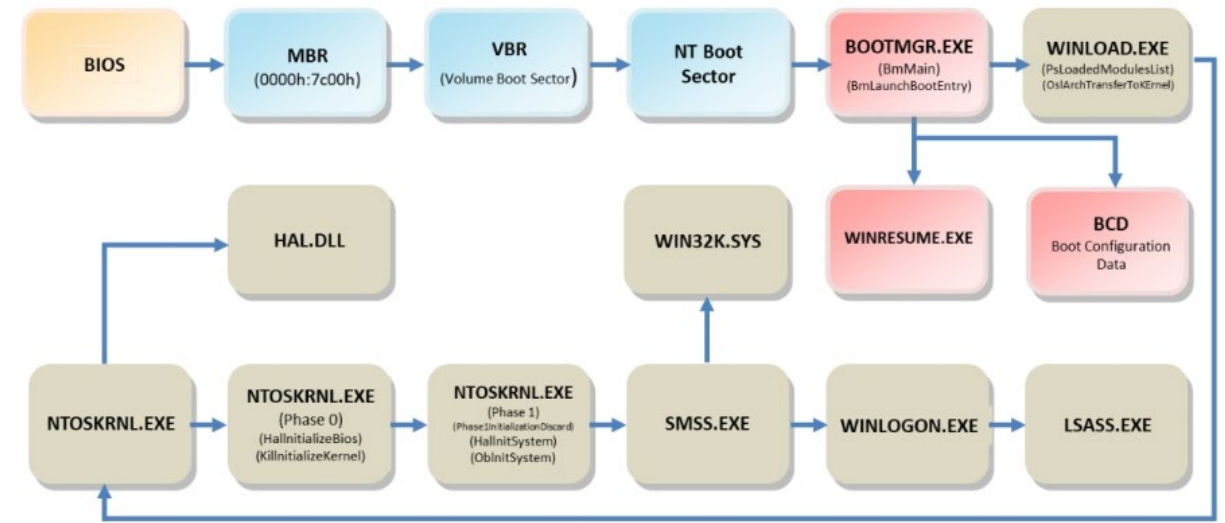
- Allows 128 partitions – MBR allows 4 partitions
- By default, all Hard Disks come with GUID Partition Table, however, you still have the option for MBR while re-formatting or re-partitioning disks

## Booting

- Booting is a process of starting/ restarting a computer
- Cold Booting/ Hard Booting
- Warm Booting

The UEFI boot process has the following **five phases**,

Security phase , Pre-EFI initialization phase, Driver Execution Environment phase, Boot Device Selection phase and Runtime phase



# Disk Partitions

## Five Phases

Security phase , Pre-EFI initialization phase, Driver Execution Environment phase, Boot Device Selection phase and Runtime phase

## Identifying the GUID Partition Table (GPT)

Get-GPT –Path [\\.\PHYSICALDRIVE0](#)

Disk formatted using the GPT partitioning scheme

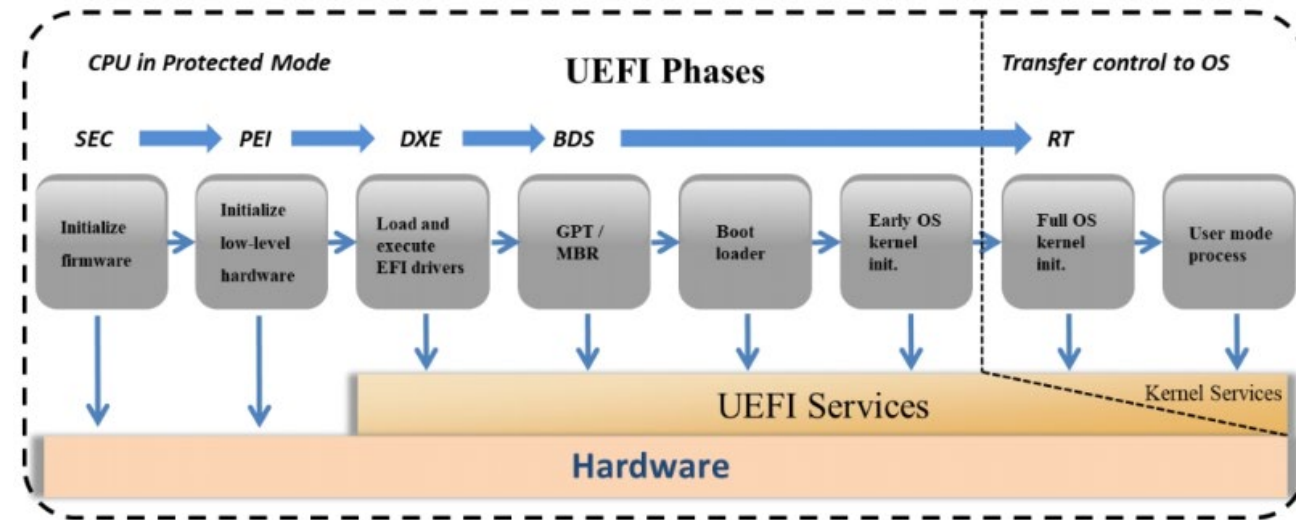
Get-BootSector –Path [\\.\](#)

Disk formatted using the MBR partitioning scheme

Get-ForensicBootSector –Path [\\.\](#)

MBR formatted Disk – Partition Table

Get-ForensicPartitionTable –Path [\\.\](#)



diskpart

detail disk

select partition=0

# File System

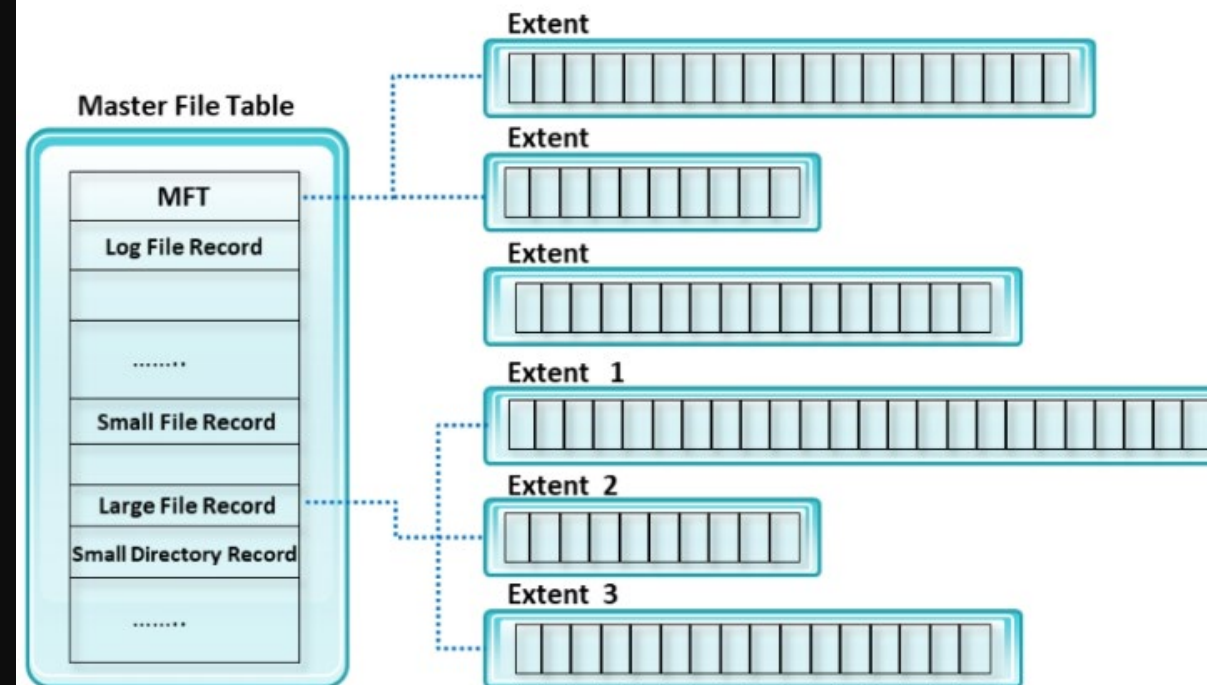
## New Technology File System (NTFS)

- Introduced with Windows NT
  - Recommended file system for Windows 2000 Pro, XP, and later versions
  - Improvements over FAT file systems
  - NTFS provides more information about a file
  - NTFS gives more control over files and folders
  - NTFS was Microsoft's move towards a journaling file system
  - In NTFS, everything written to the disk is considered a file
  - On an NTFS disk
    - **First data set is the Partition Boot Sector**
    - **Next is Master File Table (MFT)**
  - NTFS results in much less file slack space
  - Clusters are smaller for smaller disk drives
  - NTFS also uses Unicode (*An international data format*)
- ❖ MFT contains **information about all files on the disk** (*Including the system files the OS uses*)
  - ❖ In the MFT, the first 15 records are reserved for system files
  - ❖ Records in the MFT are called **METADATA**

# File System

- In the NTFS MFT, All files and folders are stored in separate records of 1024 bytes each
- Each record contains file or folder information which is further divided into record fields containing metadata
- A record field is referred to as an attribute ID
- File or folder information is typically stored in one of two ways in an MFT record: Resident and nonresident
- Files larger than 512 bytes are stored outside the MFT.
- MFT record provides cluster addresses where the file is stored on the drive's partition which is referred to as data runs
- Each MFT record starts with a header identifying it as a resident or nonresident attribute

| System File              | Filename  | MFT Record | Purpose of the File                                                                                                              |
|--------------------------|-----------|------------|----------------------------------------------------------------------------------------------------------------------------------|
| Master File Table        | \$Mft     | 0          | It contains a record of all the files and folders on an NTFS volume                                                              |
| Master File Table mirror | \$MftMirr | 1          | It contains a backup of the MFT and is used when the MFT is corrupt/damaged                                                      |
| Log file                 | \$LogFile | 2          | It stores the logs pertaining to changes in file system metadata, and is used for file system recovery in case of a system crash |
| Volume                   | \$Volume  | 3          | It contains information about the volume                                                                                         |
| Attribute definitions    | \$AttrDef | 4          | It lists attributes and their details such as names, numbers, and descriptions                                                   |
| Root filename index      |           | 5          | It is the root folder                                                                                                            |
| Cluster bitmap           | \$Bitmap  | 6          | It maintains a list of all the used and unused clusters on an NTFS volume                                                        |
| Boot sector              | \$Boot    | 7          | It includes the BPB and bootstrap code, and is essential for booting the system                                                  |
| Bad cluster file         | \$BadClus | 8          | It contains the bad clusters on a volume                                                                                         |
| Security file            | \$Secure  | 9          | It lists all the security descriptors within a volume                                                                            |
| Uppcase table            | \$Uppcase | 10         | It is used for converting lowercase characters to uppercase characters                                                           |
| NTFS extension file      | \$Extend  | 11         | It is used for various optional extensions                                                                                       |



# File System

---

- In the NTFS MFT, All files and folders are stored in separate records of 1024 bytes each
  - Each record contains file or folder information which is further divided into record fields containing metadata
  - A record field is referred to as an attribute ID
  - File or folder information is typically stored in one of two ways in an MFT record: Resident and nonresident
  - Files larger than 512 bytes are stored outside the MFT.
  - MFT record provides cluster addresses where the file is stored on the drive's partition which is referred to as data runs
  - Each MFT record starts with a header identifying it as a resident or nonresident attribute
- 

| 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                                     |
| Filename             | Stores the filename, which can be long or short                                |
| Security descriptor  | Lists the ownership and access rights to the file                              |
| 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   | Lists the version number of the volume                                         |
| Volume name          | Lists the volume label                                                         |

# File System

| Offset   | 0  | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  | A  | B  | C  | D  | E  | F  |
|----------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 035B3400 | 46 | 49 | 4C | 45 | 30 | 00 | 03 | 00 | 9B | 99 | 98 | 00 | 00 | 00 | 00 | 00 |
| 035B3410 | 02 | 00 | 01 | 00 | 38 | 00 | 01 | 80 | A8 | 01 | 00 | 00 | 00 | 04 | 00 | 00 |
| 035B3420 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 04 | 00 | 00 | 00 | A7 | 17 | 00 | 00 |
| 035B3430 | 03 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 10 | 00 | 00 | 00 | 60 | 00 | 00 | 00 |
| 035B3440 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 48 | 00 | 00 | 00 | 18 | 00 | 00 | 00 |
| 035B3450 | 62 | 16 | 9B | 68 | 0A | 7C | C9 | 01 | BC | 78 | 9D | 68 | 0A | 7C | C9 | 01 |
| 035B3460 | BC | 78 | 9D | 68 | 0A | 7C | C9 | 01 | BC | 78 | 9D | 68 | 0A | 7C | C9 | 01 |
| 035B3470 | 20 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 035B3480 | 00 | 00 | 00 | 00 | 09 | 01 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 035B3490 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 30 | 00 | 00 | 00 | 70 | 00 | 00 | 00 |
| 035B34A0 | 00 | 00 | 00 | 00 | 00 | 00 | 02 | 00 | 52 | 00 | 00 | 00 | 18 | 00 | 01 | 00 |
| 035B34B0 | 8A | 00 | 00 | 00 | 00 | 00 | 01 | 00 | 62 | 16 | 9B | 68 | 0A | 7C | C9 | 01 |
| 035B34C0 | BC | 78 | 9D | 68 | 0A | 7C | C9 | 01 | BC | 78 | 9D | 68 | 0A | 7C | C9 | 01 |
| 035B34D0 | BC | 78 | 9D | 68 | 0A | 7C | C9 | 01 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 035B34E0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 20 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 035B34F0 | 08 | 03 | 42 | 00 | 65 | 00 | 6E | 00 | 31 | 00 | 2E | 00 | 74 | 00 | 78 | 00 |
| 035B3500 | 74 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 40 | 00 | 00 | 00 | 28 | 00 | 00 | 00 |
| 035B3510 | 00 | 00 | 00 | 00 | 00 | 00 | 03 | 00 | 1A | 00 | 00 | 00 | 1A | 00 | 00 | 00 |
| 035B3520 | F4 | 7C | F1 | 27 | DF | E7 | DD | 11 | A8 | 3F | 00 | 22 | 15 | D5 | 88 | 06 |
| 035B3530 | 80 | 00 | 00 | 00 | 70 | 00 | 00 | 00 | 00 | 00 | 18 | 00 | 00 | 00 | 01 | 00 |
| 035B3540 | 54 | 00 | 00 | 00 | 18 | 00 | 00 | 00 | 41 | 20 | 63 | 6F | 75 | 6E | 74 | 72 |
| 035B3550 | 79 | 6D | 61 | 6E | 20 | 62 | 65 | 74 | 77 | 65 | 65 | 6E | 20 | 74 | 77 | 6F |
| 035B3560 | 20 | 6C | 61 | 77 | 79 | 65 | 72 | 73 | 20 | 69 | 73 | 20 | 6C | 69 | 6B | 65 |
| 035B3570 | 20 | 61 | 20 | 66 | 69 | 73 | 68 | 20 | 62 | 65 | 74 | 77 | 65 | 65 | 6E | 20 |
| 035B3580 | 74 | 77 | 6E | 20 | 63 | 61 | 74 | 73 | 2E | 0D | 0A | 42 | 65 | 6E | 6A | 61 |
| 035B3590 | 6D | 69 | 6E | 20 | 46 | 72 | 61 | 6E | 6B | 6C | 69 | 6E | 00 | 00 | 00 | 00 |
| 035B35A0 | FF | FF | FF | FF | 82 | 79 | 47 | 11 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |

- A: All MFT records start with FILE0
- B: Start of attribute 0x10
- C: Length of attribute 0x10 (value 60)
- D: Start of attribute 0x30
- E: Length of attribute 0x30 (value 70)
- F: Start of attribute 0x40
- G: Length of attribute 0x40 (value 28)
- H: Start of attribute 0x80
- I: Length of attribute 0x80 (value 70)
- J: Attribute 0x80 resident flag
- K: Starting position of resident data

A: Starting position of attribute 0x80 \$Data

B: Length of attribute 0x80 in little endian format

C: Interpreted little endian value

|          |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
|----------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 035B3530 | 80 | 00 | 00 | 00 | 70 | 00 | 00 | 00 | 00 | 18 | 00 | 00 | 00 | 01 | 00 | 00 |
| 035B3540 | 54 | 00 | 00 | 00 | 18 | 00 | 00 | 00 | 41 | 20 | 63 | 6F | 75 | 6E | 74 | 72 |
| 035B3550 | 79 | 6D | 61 | 6E | 20 | 62 | 65 | 74 | 77 | 65 | 65 | 6E | 20 | 74 | 77 | 6F |
| 035B3560 | 20 | 6C | 61 | 77 | 79 | 65 | 72 | 73 | 20 | 69 | 73 | 20 | 6C | 69 | 6B | 65 |
| 035B3570 | 20 | 61 | 20 | 66 | 69 | 73 | 68 | 20 | 62 | 65 | 74 | 77 | 65 | 65 | 6E | 20 |
| 035B3580 | 74 | 77 | 6F | 20 | 63 | 61 | 74 | 73 | 2E | 0D | 0A | 42 | 65 | 6E | 6A | 61 |
| 035B3590 | 6D | 69 | 6E | 20 | 46 | 72 | 61 | 6E | 6B | 6C | 69 | 6E | 00 | 00 | 00 | 00 |
| 035B35A0 | FF | FF | FF | FF | 82 | 79 | 47 | 11 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |

Data Interpreter  
16 Bk (±) 112

## NTFS – MFT Resident

- A: Start of nonresident attribute 0x80
- B: Length of nonresident attribute 0x80
- C: Attribute 0x80 nonresident flag
- D: Starting point of data run
- E: End-of-record marker (FF FF FF FF) for the MFT record

## NTFS – MFT Non-Resident

|          |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
|----------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 035B3CD0 | 6A | 22 | 16 | 88 | 0B | 7C | C9 | 01 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 035B3CE0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 20 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 035B3CF0 | 08 | 03 | 42 | 00 | 65 | 00 | 6E | 00 | 32 | 00 | 2E | 00 | 72 | 00 | 74 | 00 |
| 035B3D00 | 66 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 40 | 00 | 00 | 00 | 28 | 00 | 00 | 00 |
| 035B3D10 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 04 | 10 | 00 | 00 | 00 | 18 | 00 | 00 | 00 |
| 035B3D20 | F7 | 7C | F1 | 27 | DF | E7 | DD | 11 | A8 | 3F | 00 | 22 | 15 | D5 | 88 | 06 |
| 035B3D30 | 80 | 00 | 00 | 00 | 48 | 00 | 00 | 00 | 01 | 00 | 00 | 00 | 00 | 00 | 03 | 00 |
| 035B3D40 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 02 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 035B3D50 | 40 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 06 | 00 | 00 | 00 | 00 | 00 | 00 |
| 035B3D60 | 78 | 05 | 00 | 00 | 00 | 00 | 00 | 00 | 78 | 05 | 00 | 00 | 00 | 00 | 00 | 00 |
| 035B3D70 | 31 | 03 | 15 | 55 | 01 | 00 | 01 | 00 | FF | FF | FF | FF | 82 | 79 | 47 | 11 |

A

D

B

C

E

# File System

## New Technology File System (NTFS)

- When a disk is created as an NTFS file structure, **OS assigns logical clusters to the entire disk partition**
- These assigned clusters are called **logical cluster numbers (LCNs)**.
- These LCN's become the addresses that allow the **MFT to link to nonresident files** on the disk's partition

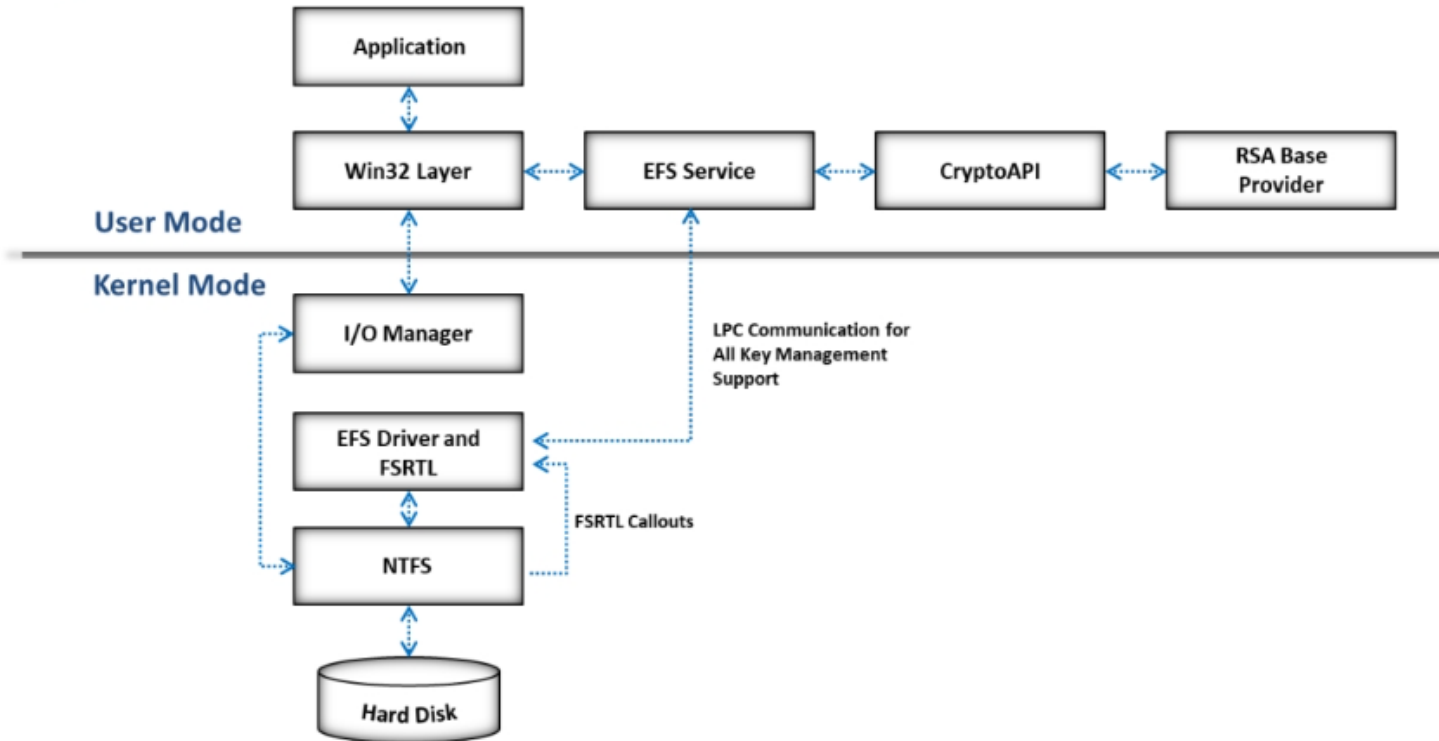
## Data streams

- Ways data can be appended to existing files
- Can obscure valuable evidentiary data, intentionally or by coincidence
- In NTFS, a data stream becomes an additional file attribute which Allows the file to be associated with different applications

# File System

## New Technology File System (NTFS)

- Compressed Files
- Encryption (EFS – Encrypting File Systems)
  - Built-in Feature
  - Uses Symmetric Key Encryption technology with Public Key Technology
  - Users can manually encrypt a file using GUI/CLI
  - The system issues a file encryption certificate whenever a user encrypts a file.
  - If the user loses that certificate and related private key, they can perform data recovery through the recovery key agent.
  - The recovery agent holds a special certificate and related private key, which help in data recovery



# File System

## New Technology File System (NTFS)

- Compressed Files
- Encryption (EFS – Encrypting File Systems)
  - Built-in Feature
  - Uses Symmetric Key Encryption technology with Public Key Technology
  - Users can manually encrypt a file using GUI/CLI
  - The system issues a file encryption certificate whenever a user encrypts a file.
  - If the user loses that certificate and related private key, they can perform data recovery through the recovery key agent.
  - The recovery agent holds a special certificate and related private key, which help in data recovery

|          |             |             |                         |                    |
|----------|-------------|-------------|-------------------------|--------------------|
| 00000000 | C8 03 00 00 | 00 00 00 00 | 01 00 00 00 00 00 00 00 | И....              |
| 00000010 | D7 4C 90 99 | 3D 90 68 42 | B4 FA DF CF E1 9E B1 D9 | ЧЛh™=hBrъЯПCh+ll   |
| 00000020 | 93 A5 51 37 | 83 A7 77 13 | 81 F7 63 AD AB 7C A9 AB | "IQ7fSw.f4c-« @«   |
| 00000030 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 00 00 00 00 | .....              |
| 00000040 | 54 00 00 00 | 54 02 00 00 | 00 00 00 00 00 00 00 00 | T...T.....         |
| 00000050 | 00 00 00 00 | 01 00 00 00 | FC 01 00 00 14 00 00 00 | .....b.....        |
| 00000060 | 80 00 00 00 | 7C 01 00 00 | 00 00 00 00 68 01 00 00 | Ъ... .....h...     |
| 00000070 | 1C 00 00 00 | 03 00 00 00 | 30 01 00 00 38 00 00 00 | .....0...8...      |
| 00000080 | 00 00 00 00 | 00 00 00 00 | 01 05 00 00 00 00 00 05 | .....              |
| 00000090 | 15 00 00 00 | 5A 56 B3 78 | 1C 36 54 29 A8 51 FF 09 | ....2Vix.6T)EQя.   |
| 000000A0 | D0 04 00 00 | 14 00 00 00 | 14 00 00 00 28 00 00 00 | P... ..(...        |
| 000000B0 | 72 00 00 00 | C8 00 00 00 | F7 C4 91 89 AD 29 24 D7 | р...И...чД'%-) \$Ч |
| 000000C0 | 78 6E 6E 9B | EE CC 64 D5 | 14 6D 71 55 36 00 35 00 | xnn>oMdX.mgU6.5.   |
| 000000D0 | 39 00 37 00 | 64 00 31 00 | 64 00 62 00 2D 00 31 00 | 9.7.d.1.d.b.-.1.   |
| 000000E0 | 63 00 32 00 | 63 00 2D 00 | 34 00 31 00 36 00 31 00 | c.2.c.-.4.1.6.1.   |
| 000000F0 | 2D 00 62 00 | 32 00 37 00 | 66 00 2D 00 32 00 65 00 | -.b.2.7.f.-.2.e.   |
| 00000100 | 66 00 31 00 | 38 00 36 00 | 65 00 39 00 36 00 64 00 | f.1.8.6.e.9.6.d.   |
| 00000110 | 65 00 63 00 | 00 00 4D 00 | 69 00 63 00 72 00 6F 00 | e.c...M.i.c.r.o.   |
| 00000120 | 73 00 6F 00 | 66 00 74 00 | 20 00 42 00 61 00 73 00 | s.o.f.t. .B.a.s.   |
| 00000130 | 65 00 20 00 | 43 00 72 00 | 79 00 70 00 74 00 6F 00 | e. .C.r.y.p.t.o.   |
| 00000140 | 67 00 72 00 | 61 00 70 00 | 68 00 69 00 63 00 20 00 | g.r.a.p.h.i.c. .   |
| 00000150 | 50 00 72 00 | 6F 00 76 00 | 69 00 64 00 65 00 72 00 | P.r.o.v.i.d.e.r.   |
| 00000160 | 20 00 76 00 | 31 00 2E 00 | 30 00 00 00 4F 00 55 00 | .v.1...0...O.U.    |
| 00000170 | 3D 00 45 00 | 46 00 53 00 | 20 00 46 00 69 00 6C 00 | =.E.F.S. .F.i.l.   |
| 00000180 | 65 00 20 00 | 45 00 6E 00 | 63 00 72 00 79 00 70 00 | e. .E.n.c.r.y.p.   |
| 00000190 | 74 00 69 00 | 6F 00 6E 00 | 20 00 43 00 65 00 72 00 | t.i.o.n. .C.e.r.   |
| 000001A0 | 74 00 69 00 | 66 00 69 00 | 63 00 61 00 74 00 65 00 | t.i.f.i.c.a.t.e.   |
| 000001B0 | 2C 00 20 00 | 4C 00 3D 00 | 45 00 46 00 53 00 2C 00 | ,. .L.=.E.F.S.,.   |
| 000001C0 | 20 00 43 00 | 4E 00 3D 00 | 6F 00 6C 00 65 00 67 00 | .C.N.=.o.l.e.g.    |
| 000001D0 | 61 00 00 00 | EB 11 78 3E | 0E 4B 72 0A 65 80 08 24 | a...л.x>.Kr.eP.\$  |
| 000001E0 | 86 08 C4 43 | 73 C3 5D 1A | 6F 77 76 8D 7C DC F5 C1 | †.HCsГ].owvK BxB   |
| 000001F0 | 44 25 55 4C | C5 15 84 39 | 32 BD B0 50 63 4A 0E C3 | D%ULE.,,92S°PcJ.Г  |
| 00000200 | 32 BC C4 A3 | 28 6D 29 D3 | C6 71 DA AA 56 8E 5F 02 | 2jDJ(m)YЖqbeVh.    |
| 00000210 | AE 66 D7 22 | 17 D0 D1 AD | 5C EF D1 A2 83 19 0A 3E | @f4".PC-\nCŸf.>    |
| 00000220 | 4E 9A 3E 7C | 74 66 E5 AD | C5 D1 26 41 04 E7 1E BD | Nx> tfe-EC&A.з.S   |
| 00000230 | 6C C0 5C 39 | C2 F6 32 28 | A5 25 4A AD 42 BF 10 5F | lA\9Bu2(I%J-Bi._   |
| 00000240 | 70 5C 9D 6E | 34 09 25 25 | 1B 53 4D D8 2E F2 38 2D | p\kn4.%%.SMIII.t8- |
| 00000250 | 7F 49 28 52 | 01 00 00 00 | 6C 01 00 00 14 00 00 00 | CI(R...l.....      |

# File System

## New Technology File System (NTFS)

- Deleting a File
  - When a file is deleted, the OS renames it and moves it to the Recycle Bin
  - Can use the Del (delete) MS-DOS command to eliminate the file from the MFT listing in the same way FAT does
- Registry
  - A database that stores hardware and software configuration information, network connections, user preferences, and setup information
  - For investigative purposes, the Registry can contain valuable evidence
    - Registry
    - Registry Editor
    - HKEY
    - Key
    - Subkey
    - Branch
    - Value
    - Default value and Hives

# Activity – for the Group!!!

**Identify and discuss the Linux and Macintosh boot process with suitable flow diagrams and examples.**

**Use the existing images in our shared folder to analyse and discuss Windows File System**

- **FAT File System Layout**
- **FAT Partition Boot Sector**
- **FAT Folder Structure**
- **NTFS Architecture**
- **NTFS Master File Table**



Prifysgol Cymru  
Y Drindod Dewi Sant  
University of Wales  
Trinity Saint David

200  
1822 - 2022

# Any Questions?

***Digital Forensics***  
*(ACCA7031)*

Applied Computing - WISA

*Man Geni Addysg Uwch yng Nghymru*  
*Where Higher Education Began in Wales*

[www.uwtsd.ac.uk](http://www.uwtsd.ac.uk)



Prifysgol Cymru  
Y Drindod Dewi Sant  
University of Wales  
Trinity Saint David

200  
1822 - 2022

# References

- EC Council – CHFI V10 Ebook
- Bossler, Adam M.\_ Holt, Thomas J.\_ Seigfried-Spellar, Kathryn C – Cybercrime and digital forensics\_ an introduction-Routledge (2017\_2018)
- Digital Forensics and Incident Response:  
A practical guide to deploying digital forensic techniques in response to cyber security incidents
- Jason Sachowski - Digital Forensics and Investigations – People, Process, and Technologies to Defend the Enterprise
- Whitcomb, C. (2007). The evolution of digital evidence in forensic science laboratories. The Police Chief, 74(11).

*Man Geni Addysg Uwch yng Nghymru*  
*Where Higher Education Began in Wales*

[www.uwtsd.ac.uk](http://www.uwtsd.ac.uk)

***Digital Forensics***  
***(ACCA7031)***

**Applied Computing - WISA**