

Prepared by Dr. Nermin Ewais

CYB 770
IT Forensics

Lecture 03



Exploring evidence And Data Acquisition

Lecture 03

CYB 770
IT Forensics

Prepared by
Dr. Nermin Ewais

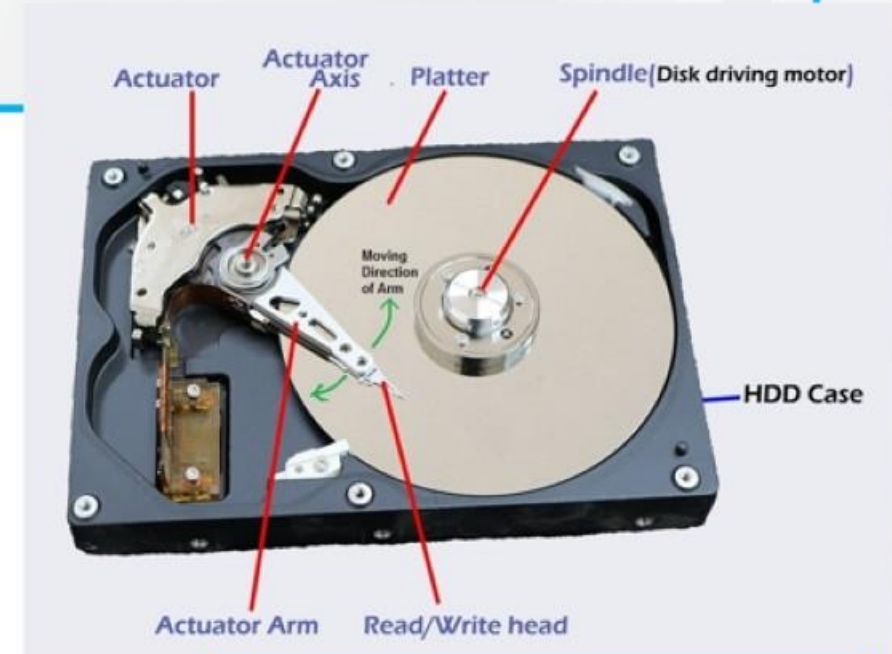
- Exploring evidence
- Disk Drive
- Data Acquisition

Law matter produced before a court of law in an attempt to prove or disprove a point in issue, such as the statements of witnesses, documents or material objects.

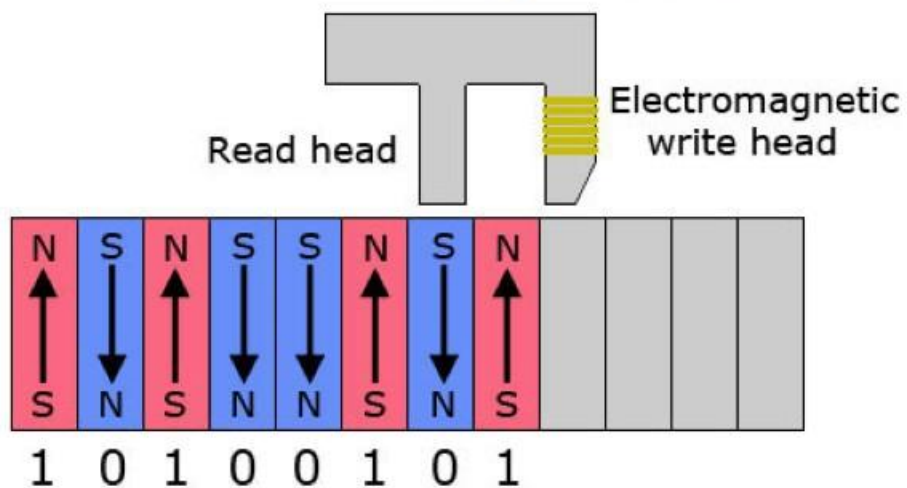
Disk Drive

- Magnetic storage devices
 - Magnetic storage devices read and write data by using electromagnetic read/write heads (floppy and magnetic tap)
- Optical storage devices
 - CD/DVD
- Flash Memory Device

- HDD
 - Capacity of hard disk
 - Several disks known as platters
 - (sector and tracks)
 - Data is read, written or erased as the magnetic dots pass under read/write heads
 - (seek time , access time , transfer time)
- SSD
 - Data is stored by controlling the movement of electrons within a NAND chip
 - Data is stored as 0s and 1s in millions of tiny transistors within the chip



Hard drive read/write head



Hard Drive Cabels

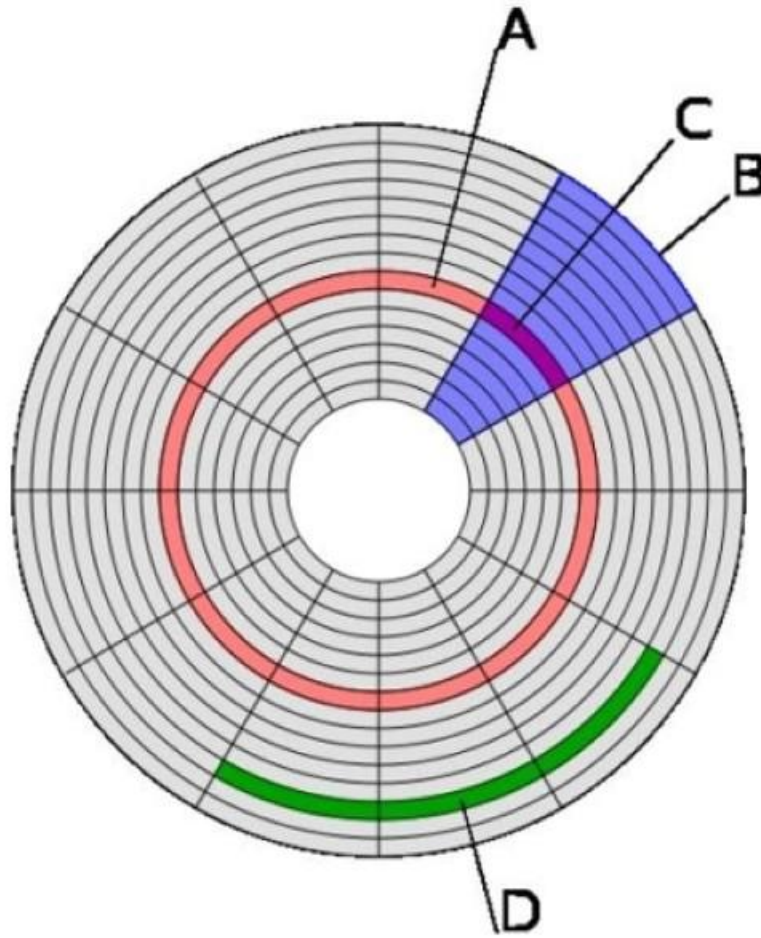
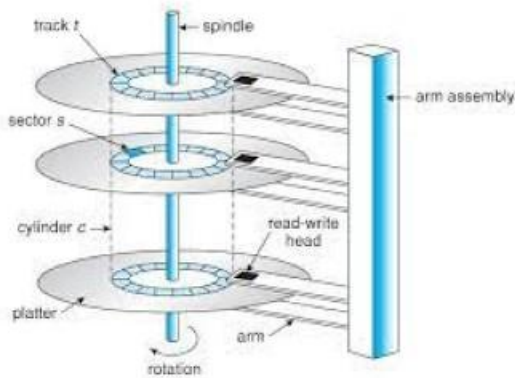


IDE(PATA)



SATA

Hard Drive Structure



Hard Drive Structure:

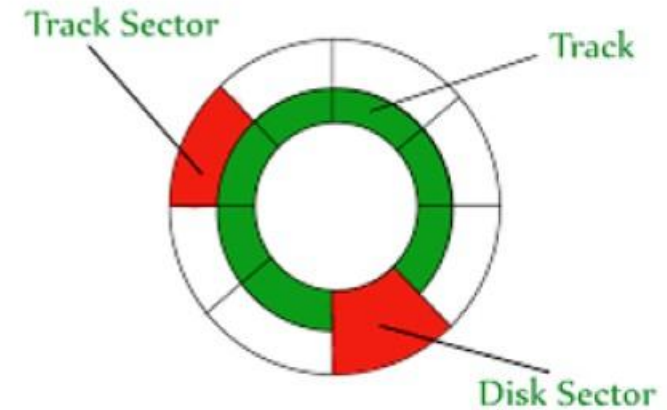
A = track

B = sector

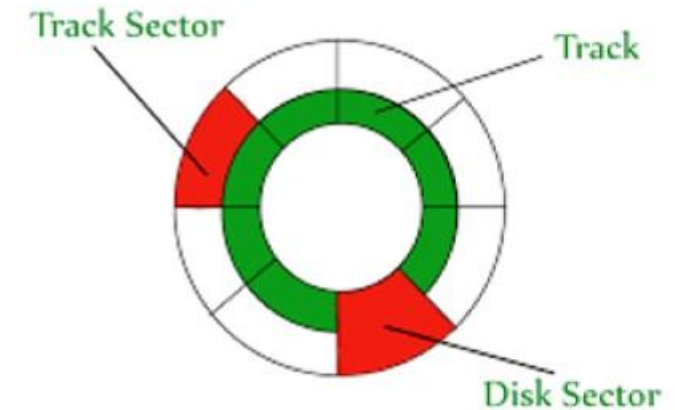
C = sector of a track

D = cluster

- Track : Disk platters are formatted in a system of concentric circles, or rings, called tracks.
- Sector : Within each track are sectors, which subdivide the circle into a system of arcs, each formatted to hold the same amount of data—typically 512 bytes



- **Bad Sector :** Bad sectors refer to areas on the disk where data cannot be appropriately accessed due to logical or physical errors.

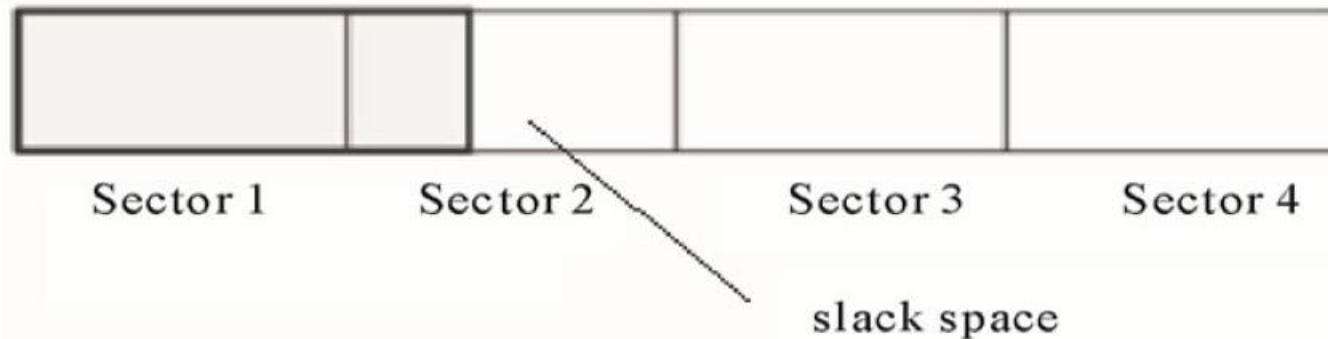


- **Sector is used but not allocated**

Unallocated Space

One of the most neglected areas in forensic data recovery is that of unallocated Space. When a file on a hard drive containing data is deleted, the data belonging to the file remains on the disk. This area is known as unallocated space. The data will remain there until it is overwritten by another file. Any data found in this area at one time belonged to a file which has since been deleted.

- **Slack space** is the leftover storage that exists on a computer's hard disk drive when a computer file does not need all the **space** it has been allocated by the operating system.
- The examination of **slack space** is an important aspect of computer forensics.



- Understanding Storage Formats for Digital Evidence
- Understanding write blocking
- Data Acquisition Types
- Data Acquisition Methods
- Defining forensic imaging

Understanding Storage Formats for Digital Evidence

- Data in a forensics acquisition tool is stored as an image file
- Each vendor has unique features, so several different proprietary formats are available.
- Depending on the proprietary format, many forensics analysis tools can read other vendors' formatted acquisitions.

- Bit Stream

- Bit Stream (mirror image/ evidence grade backups) involves capturing data on the copied media.
- This include hidden and residual data (slack, space , swap, unused space, residue, deleted files , etc.)

- Backup

- Slack, residue , deleted ,etc.. Are not indexed .
- Backup usually donot capture this data they modify the timestamps of data contaminating the timeline .

- Three formats
 - Raw format
 - Proprietary formats
 - Advanced Forensics Format (AFF)

- Examiners performed a bit-by-bit copy from one disk to another disk the same size or larger.
- Makes it possible to write bit-stream data to files.
- This copy technique creates simple sequential flat files of a suspect drive

or data set. The output of these flat files is referred to as a **raw format**.

- Advantages
 - Fast data transfers
 - Ignores minor data read errors on source drive
 - Most computer forensics tools can read raw format
- Disadvantages
 - Requires as much storage as original disk or data
 - Tools might not collect marginal (bad) sectors

- Most commercial forensics tools have their own formats for collecting digital evidence.

Proprietary formats typically offer several features that complement the vendor's analysis.

- Features offered
 - Option to compress or not compress image files
 - Can split an image into smaller segmented files
 - Can integrate metadata into the image file

- Disadvantages
 - Inability to share an image between different tools
 - File size limitation for each segmented volume
 - The Expert Witness format is unofficial standard

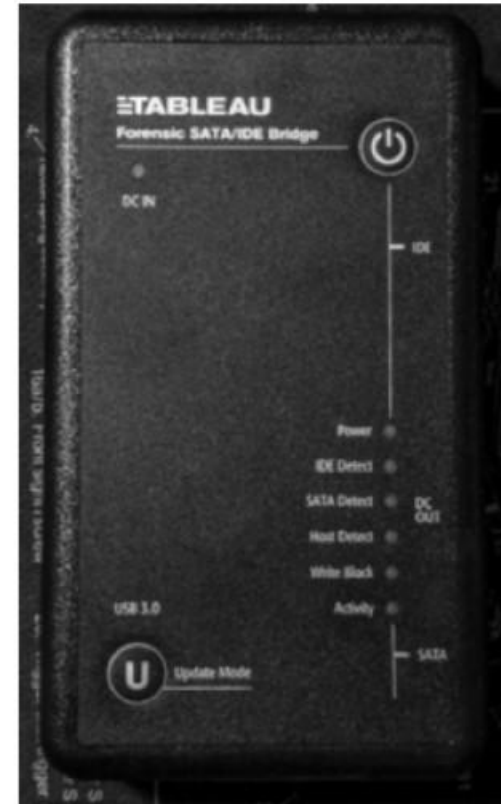
- Developed by Dr. Simson L. Garfinkel as an open-source acquisition format
- Design goals
 - Provide compressed or uncompressed image files
 - No size restriction for disk-to-image files
 - Provide space in the image file or segmented files for metadata
 - Simple design with extensibility
 - Open source for multiple platforms and OSs

- Design goals
 - Internal consistency checks for self-authentication
- File extensions include .afd for segmented image files and .afm for AFF metadata

Understanding write blocking

- We want to ensure we do not change a single bit of data on the source device.
- To prevent the alteration of the source device, we must use a write blocker.
- You have a choice of utilizing a "hardware write blocker" or a "software write blocker."

- A hardware write blocker is a device that intercepts and prevents any modification to the source device.

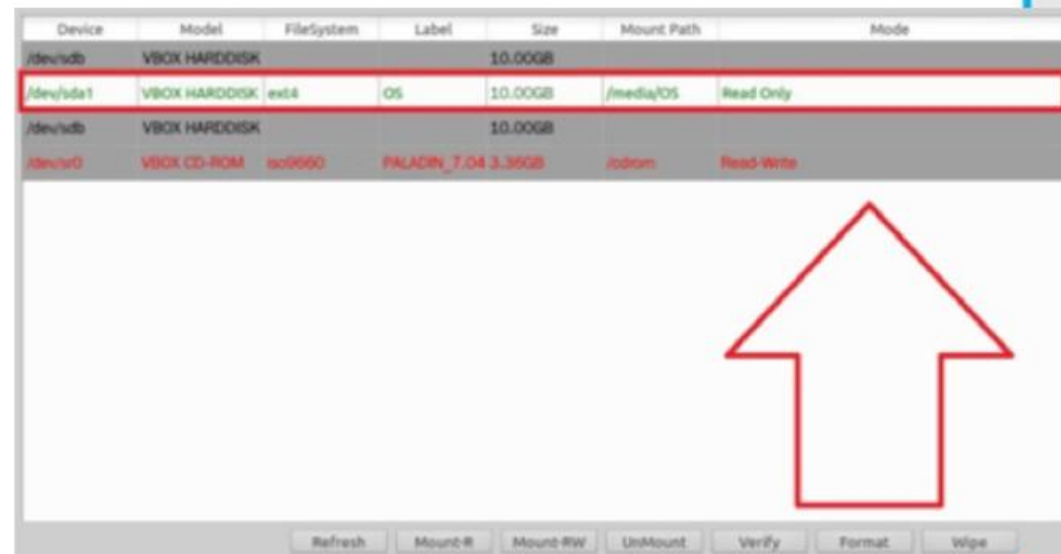


- Software write blocking is where a change is made to the operating system to stop it from making writes to the device.
- For a Windows based system, there is a registry change you can make to prevent rights to attached USB devices.
- This will require you to have a hard drive dock to connect to the system.

Paladin toolbox

There are two options when you mount a device:

- Read-only
- Read/write
- You **should not mount** a device read/write unless you want to change the device.
- If you create a **forensic image of the device**, then you should mount read-only.



Data Acquisition Types

Two types of data **acquisition**

- Static acquisition
- Live acquisition

- **Static acquisition**

- Static data acquisition refers to the process of extracting and gathering the **unaltered data from storage media**.
- Sources of non-volatile data include hard drives, DVD-ROMs, USB drives, flash cards, smart-phones, external hard drives, etc.
- Copying a hard drive from a powered-off system
- Used to be the standard
- Does not alter the data, so it's repeatable

- **Static acquisition: Steps (for laptop as Example):**
- **Step 1: Power Off the Laptop**
- Turn off the suspect computer properly to prevent any further data changes.
- **Step 2: Remove the Storage Device**
- Physically remove the hard drive (HDD or SSD) from the laptop.
- **Step 3: Connect via Write-Blocker**
- Attach the suspect's drive to the forensic workstation through a **write-blocker** to prevent accidental writing.

- **Static acquisition: Example using FTK Imager (GUI):**
 - Launch FTK Imager
 - Choose **Create Disk Image**
 - Select the **Physical Drive**
 - Choose output format (e.g., E01)
 - Enter case info and hash options
 - Start acquisition

- **Live acquisition**

- A live acquisition is where data is retrieved from a digital device directly via its normal interface; for example, switching a computer on and running programs from within the operating system. This has some level of risk, as data is likely to be modified.
- Copying data from a running computer
- Now the preferred type, because of hard disk encryption
- Cannot be repeated exactly—alters the data
- Also, collecting RAM data is becoming more important
 - But RAM data has no timestamp, which makes it much harder to use

- **Live acquisition : When Live Acquisition is Used**
- The system **cannot be powered off** (e.g., a server or ransomware case).
- You need **volatile evidence** (like RAM contents or encryption keys).
- Suspect may have **encrypted drives** — if you shut down, you lose access.

- **Live acquisition: Steps**

- **Step 1: Prepare the Forensic USB**
- Investigator brings a trusted USB containing forensic tools.
- **Step 2: Plug USB into Target System (running)**
- No installation — run tools **directly from USB**.
- **Step 3: Capture Volatile Data**
 - **Example D – FTK Imager Live**
Open FTK Imager → “Capture Memory” → Save .mem file → Optionally include pagefile (pagefile.sys).
- **Step 4: Optionally Acquire a Disk Image (While Running)**
- If safe, use FTK Imager to image the system disk (logical acquisition) while it's live.

- **Live acquisition: Why Live Acquisition is Important**

Evidence Type	Example
Volatile Memory	RAM contents (running malware, encryption keys, passwords)
Active Network	IP connections, open ports
Running Processes	Malware, ransomware, keyloggers
User Activity	Logged-in users, clipboard data

Static vs. Live

Feature	Static Acquisition	Live Acquisition
Power State	System off	System on
Captures Volatile Data	No	Yes
Risk of Data Change	Low	Higher
Common Tools	FTK Imager, dd	FTK Imager Live, DumpIt, Volatility
Use Case	Hard drive imaging	Memory, network, encryption analysis

- **Order of volatility**
 - ▣ Registers and Cache
 - ▣ Routing Table, ARP Cache, Process Table, Kernel Statistics
 - ▣ Contents of System Memory (RAM)
 - ▣ Remote Logging and Monitoring Data
 - ▣ Physical Configuration, Network Topology
 - ▣ Temporary File Systems
 - ▣ Data on Disk
 - ▣ Archival Media

Data Acquisition Methods

- When making a copy, consider:
 - Size of the source disk
 - Use digital signatures for verification
 - When working with large drives, an alternative is using tape backup systems whether you can retain the disk

Methods of data collection

- Creating a disk-to-image file
- Creating a disk-to-disk
- Creating a logical disk-to-disk or disk-to-data file

Or Creating a sparse data copy of a file or folder

- Creating a disk-to-image file
 - Most common method and offers most flexibility
 - Can make more than one copy
 - Copies are bit-for-bit replications of the original drive
 - ProDiscover, EnCase, FTK, SMART, Sleuth Kit, X-Ways, iLookIX

- Creating a disk-to-disk
 - When can't make a disk-to-image file because of hardware or software errors or incompatibilities Or acquire older drives
 - Several imaging Tools can copy data exactly from an older disk to a newer disk
 - Tools can adjust disk's geometry configuration (its cylinder, head, and track configuration)
 - EnCase, SafeBack, SnapCopy

- Logical acquisition or sparse acquisition
 - Can take several hours; use when your time is limited
 - Logical acquisition captures only specific files of interest to the case
 - Sparse acquisition collects fragments of unallocated (deleted) data
 - For large disks
 - PST or OST mail files, RAID servers

Defining forensic imaging

Defining forensic imaging

- We never want to change the source device/digital evidence
- You should only conduct your digital forensic analysis on a copy and not the original.
- Remember the forensic copy you make will also be considered the evidence and will have the same responsibilities as the original source device in terms of evidence.

- We are creating a bit-for-bit copy of the source device, but we store that data in a forensic image format.
- This could be a DD image, an E01 image, or an AFF image.
- We take that source data and wrap it in a protective wrapper of the forensic image.
- We will recover deleted files, file slack, and partition slack.

Logical forensic image

- Sometimes, we are restricted to only accessing specific datasets. They do not allow us to access the entire container.
- We cannot create a bit-for-bit copy of a forensic image or a forensic copy.
- This could be when we are extracting data from a server, and we cannot shut the server down to create a forensic image from the source hard drives.
- Due to this, we can make logical copies of the files and folders pertinent to the investigation.
- We will NOT be able to recover deleted files, file slack, and partition slack.

- Create a duplicate copy of your evidence image file
- Make at least two images of digital evidence
 - Use different tools or techniques
- Copy **host protected area** of a disk drive as well
 - Consider using a hardware acquisition tool that can access the drive at the BIOS level
- Be prepared to deal with encrypted drives
 - **Whole disk encryption** feature in Windows called BitLocker makes static acquisitions more difficult
 - May require user to provide decryption key

- Autopsy
- Easeuse
- WinHex

Chapter 03

Autopsy

123 - Autopsy 4.14.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Timeline File Discovery Close Case Generate Report

Keyword Lists Keyword Search

Listing

Data Sources

Table Thumbnail

Save Table as CSV

Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone	Device ID
1.001	Image	4871301120	512	Asia/Calcutta	b11b5051-2bf4-4cf2-a318-a10c4025f3c3

Hex Text Application Message File Metadata Context Results Annotations Other Occurrences

Name	/img_1.001
Type	Raw Single
Size	4871301120
MD5	aee4fcd9301c03b3b054623ca261959a
SHA1	da2fe30fe21711edf42310873af475859a68f300
SHA256	65e2002fed0b286f49541c7e97dcec0dda913d51a063ceeed86782bdacda2312
Sector Size	512
Time Zone	Asia/Calcutta
Acquisition Details	Unknown
Device ID	b11b5051-2bf4-4cf2-a318-a10c4025f3c3

xpinbox1 - Autopsy 3.0.0b3

File Edit View Tools Window Help

Close Case Add Image Generate Report

Keyword Lists Search...

Directory Listing
xp-sp3-v4.001\vol2

Table View Thumbnail View

Name	Mod. Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags
\$Boot	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	8192	Allocated	Allocated
\$Extend	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	344	Allocated	Allocated
\$LogFile	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	23085056	Allocated	Allocated
\$MFT	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	15859712	Allocated	Allocated
\$MFTMirr	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	4096	Allocated	Allocated
\$Secure:\$SDS	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	0	Allocated	Allocated
\$UpCase	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	131072	Allocated	Allocated
\$Volume	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	0	Allocated	Allocated
AUTOEXEC.BAT	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	0	Allocated	Allocated
boot.ini	2012-01-20 17:19:25	2012-01-20 17:20:54	2012-01-20 17:19:25	2012-01-20 12:10:10	211	Allocated	Allocated
CONFIG.SYS	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	0	Allocated	Allocated
Documents and Settings	2012-03-22 19:29:54	2012-03-22 19:29:54	2012-03-10 14:40:46	2012-01-20 12:10:41	56	Allocated	Allocated
IO.SYS	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	0	Allocated	Allocated
MSDOS.SYS	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	0	Allocated	Allocated
NTDETECT.COM	2008-04-13 22:13:04	2012-01-20 12:11:07	2012-01-20 12:10:07	2008-04-13 22:13:04	47564	Allocated	Allocated
ntldr	2008-04-14 00:01:44	2012-01-20 12:11:07	2012-01-20 12:10:07	2008-04-14 00:01:44	250048	Allocated	Allocated
pagefile.sys	2012-03-10 14:44:29	2012-03-10 14:44:29	2012-03-10 14:44:29	2012-01-20 12:09:08	20971520	Allocated	Allocated
Program Files	2012-03-20 19:25:02	2012-03-20 19:25:02	2012-03-10 14:40:46	2012-01-20 12:11:01	56	Allocated	Allocated
System Volume Information	2012-01-20 17:21:37	2012-01-20 17:21:37	2012-03-10 14:40:46	2012-01-20 12:10:41	56	Allocated	Allocated
WINDOWS	2012-03-05 19:12:38	2012-03-05 19:12:38	2012-03-10 14:40:46	2012-01-20 12:09:08	56	Allocated	Allocated
\$OrphanFiles	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated

Result View Hex View Media View String View Text View

Page: 1 of 3 Page Go to Page:

```
0x00000000: 66 55 66 39 EC 66 FD E5 FF FF 00 00 1E 06 66 53 EUE..E.....E8
0x00000010: 66 56 66 57 B9 FD A4 C1 E9 04 52 C8 03 C1 7D D8 EUEW.....
0x00000020: 7D C0 66 39 CC 66 30 0E 00 00 52 D1 30 0E 04 00 ..E.E.....
0x00000030: 66 39 5E 08 66 39 4E 0C 66 39 76 10 66 39 7E 14 E..E.N.E.v.E..
0x00000040: 66 39 56 18 66 39 6E 1C 7D D0 66 BC 06 10 00 00 E.V.E.n.E.....
0x00000050: 66 55 66 52 66 57 66 56 66 51 66 53 66 33 C0 66 EUREWEVEQES.E
0x00000060: 33 DB 66 33 C9 66 33 D2 66 33 F6 66 33 FF E8 B7 3.E3.E3.E3.E3..
0x00000070: 02 66 0F B2 26 00 00 66 5F 66 5E 66 5B 07 1F 66 E..E.E.E.E..E
0x00000080: 5D CB 00 00 00 00 00 00 00 00 00 00 00 00 00 00 }.....
0x00000090: 55 39 EC 56 57 53 60 4E 06 B8 00 D8 CD 15 53 39 U..VWS.N...S.
0x000000A0: 5E 04 C6 27 C6 47 01 58 C6 67 02 C6 47 03 30 4F ^..G.K.g..G..O
0x000000B0: 04 C6 77 06 C6 57 07 30 7F 08 30 77 0A 5B 5F 5E .w.W.....V..^
0x000000C0: 5D C3 55 39 EC 56 B8 01 D8 60 4E 06 60 6E 08 39 }U..V...N..n..
0x000000D0: 76 04 CD 15 60 C4 5E 5D C3 06 53 B8 00 F0 7D C0 V.....S.....
```



Thank You