Windows Disk Forensics

Understanding how digital evidence lives on disks

0x251e

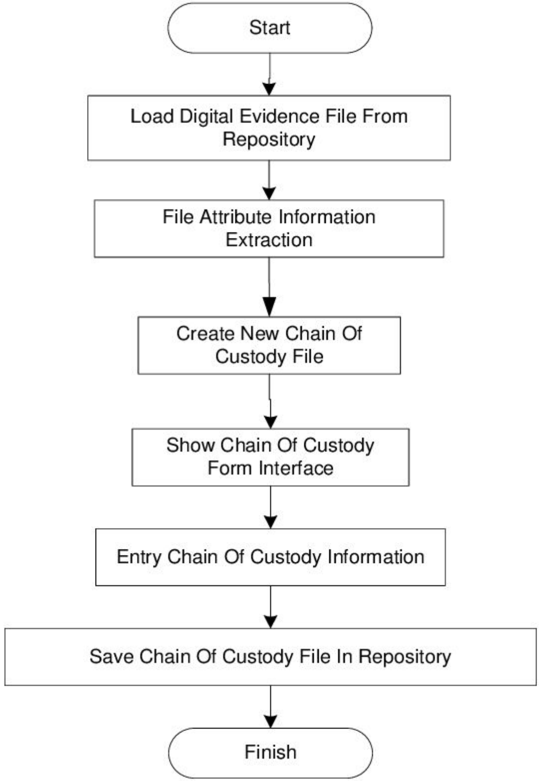
What Is Disk Forensics?

Definition: Examining digital storage media for evidence

Real-world uses:

- Investigating data breaches
- Recovering deleted files
- Analyzing malware persistence

Digital forensic process (acquire → preserve → analyze → report)


Start
Load Digital Evidence File From Repository
File Attribute Information Extraction
Create New Chain Of Custody File
Show Chain Of Custody Form Interface
Entry Chain Of Custody Information
Save Chain Of Custody File In Repository
Finish

How Data Is Stored

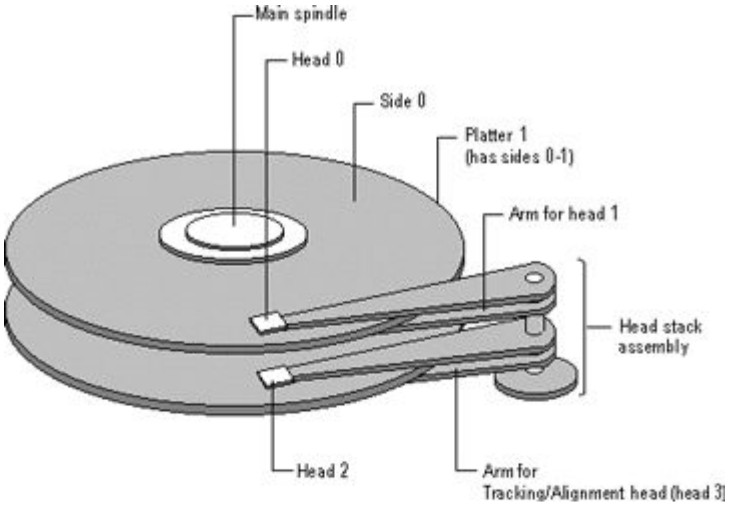
Physical Components

Platters: Circular disks coated with magnetic material (like CDs stacked together)

Read/Write Heads: Tiny arms that hover nanometers above platters

Spindle Motor: Spins platters at 5,400-15,000 RPM

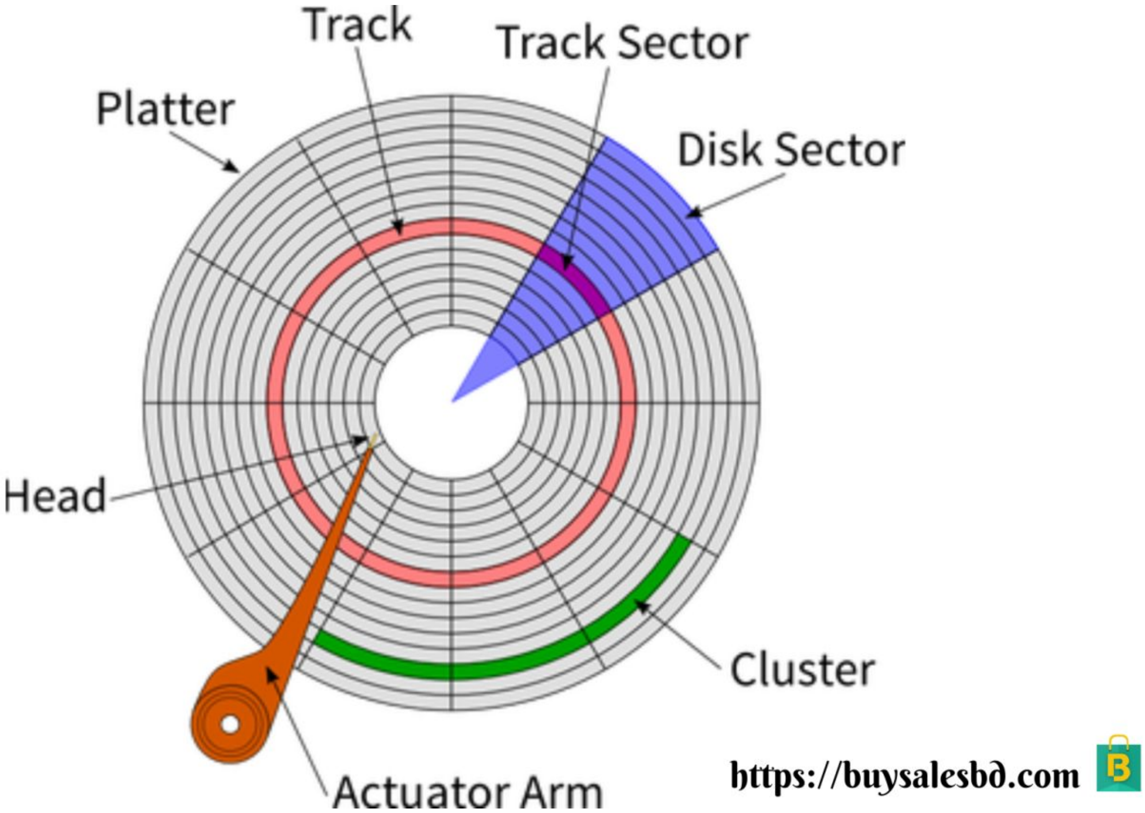
Actuator Arm: Moves heads across the platter surface



Data Storage Method

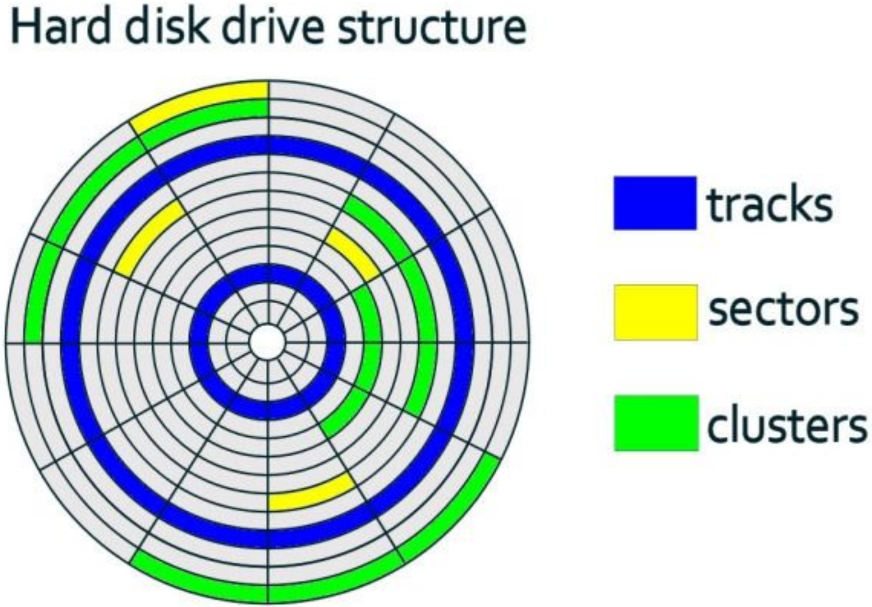
- **Binary System**: All data stored as 1s and 0s (bits)
- **Magnetic Polarization**:
  - North pole = 1
  - South pole = 0
- Tiny magnetic regions on platter surface represent each bit

How Data Is Stored



How Data Is Stored

- **Tracks**: Concentric circles on the platter
- **Sectors**: Pie-slice divisions (typically 512 bytes or 4KB each)
- **Clusters**: Groups of sectors treated as units
- File system keeps a map of where each file's data is located



Windows File Systems

FAT32 (File Allocation Table 32)

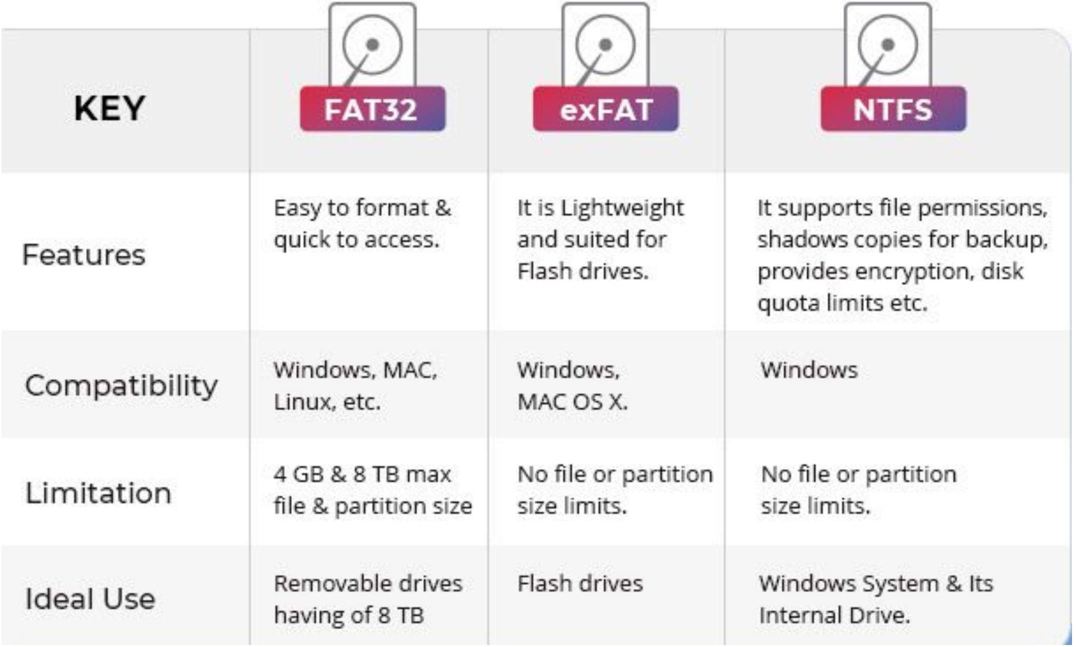
- Max file size: 4GB
- Max partition size: 8TB, but best at 2TB

exFAT (Extended FAT)

- Max file size:: 16 exabytes
- Max partition size: 128 petabytes
- Advantages: No 4GB limit, simpler than NTFS, optimized for flash drives

NTFS (New Technology File System)

- Max File Size: 16 exabytes
- Max Partition Size: 8 petabytes
- Features:
    - File permissions and security
    - Encryption support
    - Compression
    - Journaling (crash protection)
    - Shadow copies/backups



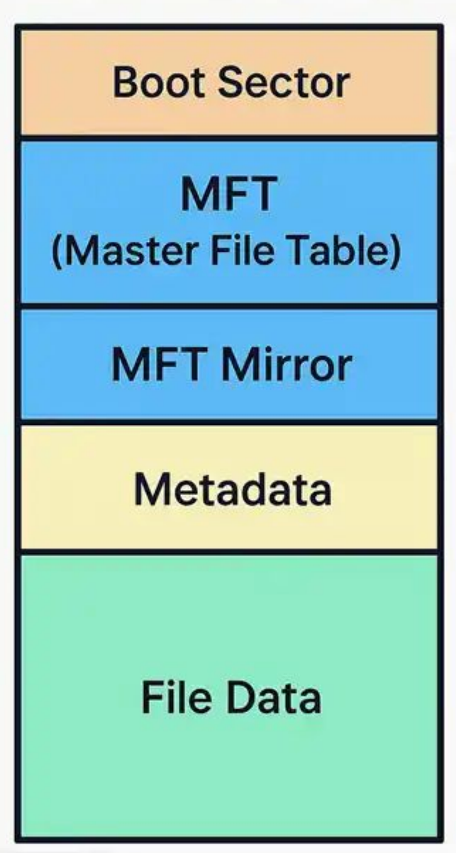
KEY	FAT32	exFAT	NTFS
Features	Easy to format & quick to access.	It is Lightweight and suited for Flash drives.	It supports file permissions, shadows copies for backup, provides encryption, disk quota limits etc.
Compatibility	Windows, MAC, Linux, etc.	Windows, MAC OS X.	Windows
Limitation	4 GB & 8 TB max file & partition size	No file or partition size limits.	No file or partition size limits.
Ideal Use	Removable drives having of 8 TB	Flash drives	Windows System & Its Internal Drive.

Need compatibility? → FAT32
Large files + portability? → exFAT
Windows system/internal drive? → NTFS

Inside of NTFS

MFT (Master File Table)

- The heart of NTFS - database of all files and folder
- Each files gets a record, usually 1 KB
- Contains file metadata and location
- First 16 records reserved for system files
- Located at the beginning of volume



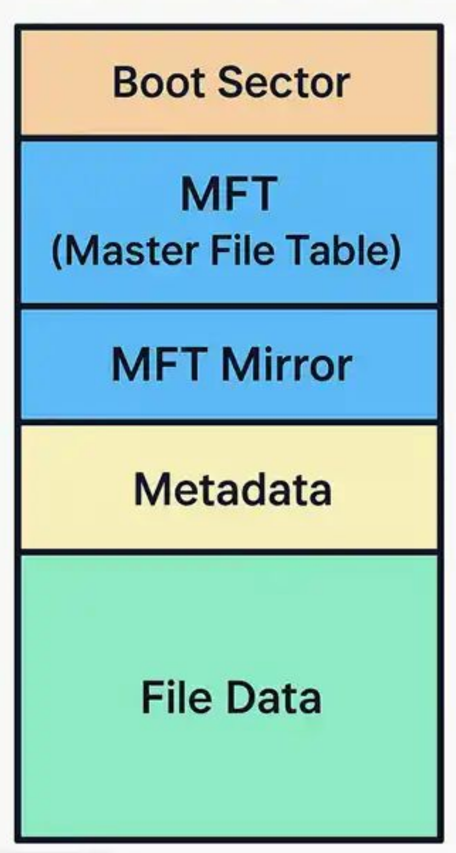
Inside of NTFS

File Records:

- Each entry in the MFT
- Contain file attributes
- Small files stored entirely in MFT
- Large files point to data cluster
- Includes timestamps,permissions, size

Attributes:

- **$STANDARD_INFORMATION**: timestamps, flags
- **$FILE_NAME**: name and parent directory
- **$DATA**: actual file content
- **$SECURITY_DESCRIPTOR**: permissions
- Everything is an attribute in NTFS



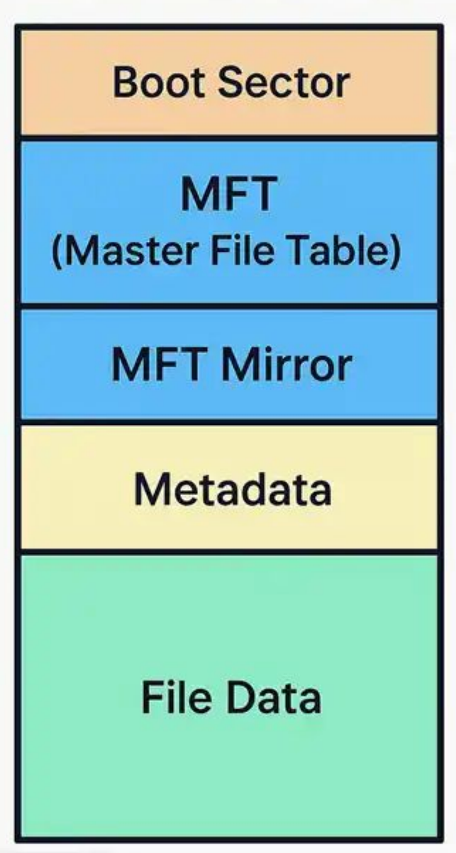
Inside of NTFS

$Bitmap

- Tracks free and used clusters
- Each bit represents one cluster
- 1 = cluster in use
- 0 = cluster available
- Helps quickly find free space

$LogFile

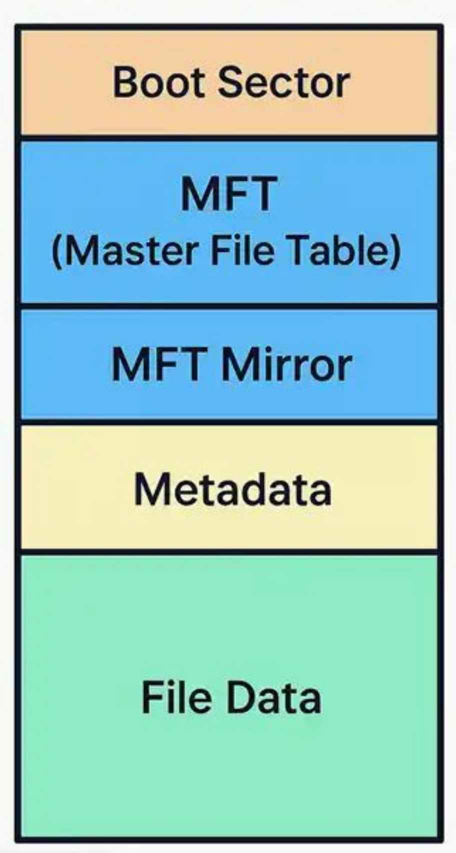
- Transaction journal for crash recovery
- Records all metadata changes
- Enables quick recovery after crashes
- Prevents file system corruption
- Circular buffer that overwrites old entries



Inside of NTFS

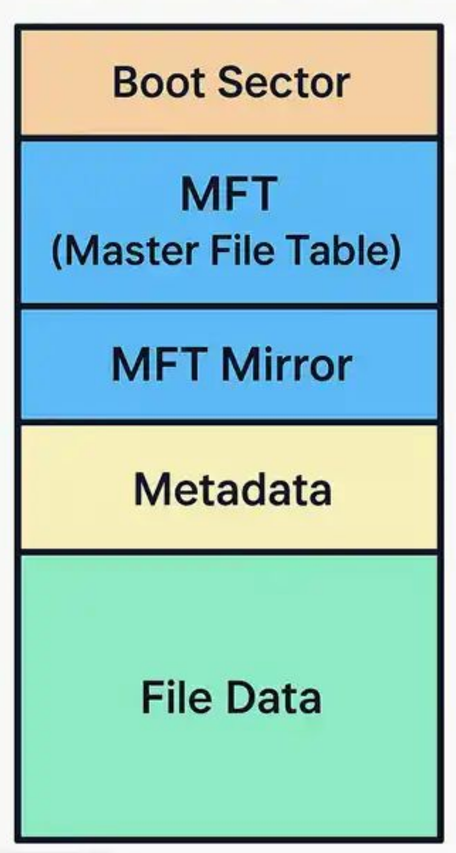
Other Key Files

- **$Boot**: boot sector information
- **$Volume**: volume information
- **$BadClus**: tracks bad sectors
- **$Secure**: security descriptors
- All begin with $ and are hidden

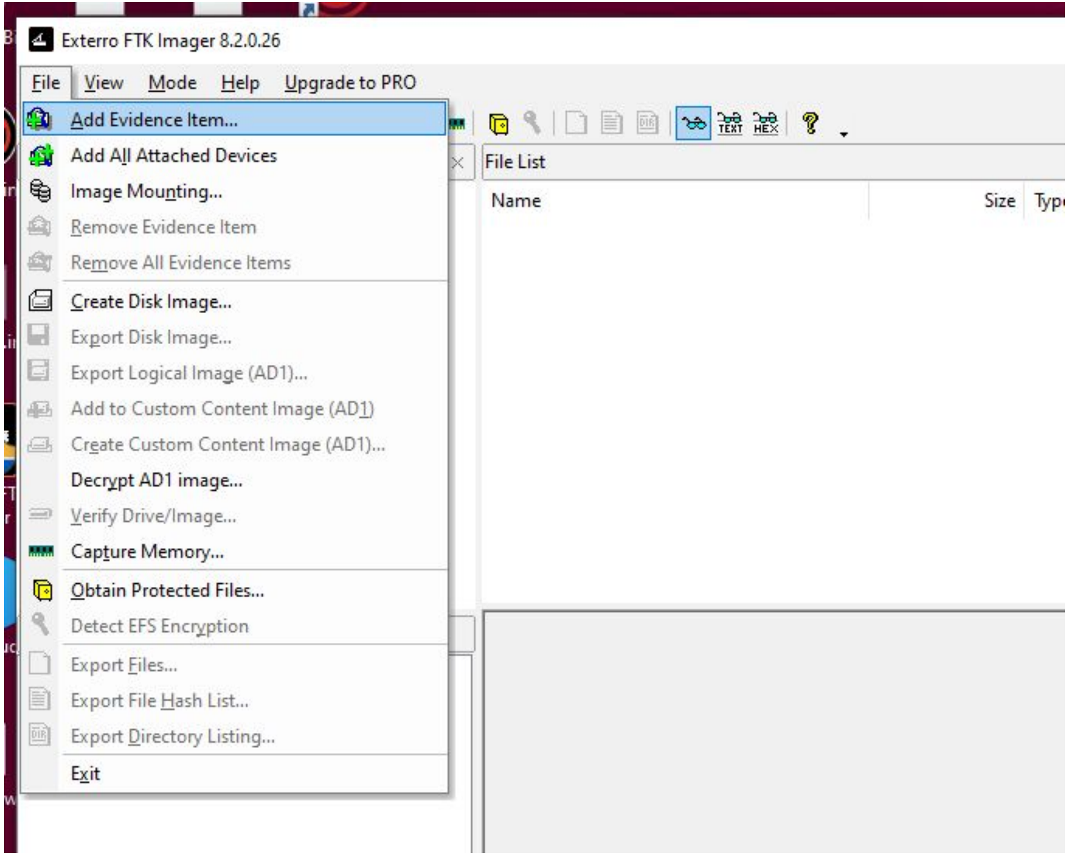


MFT Explained

- Each file = one MFT entry
- Stores:
  - Filename
  - MAC timestamps (Modified, Accessed, Created)
  - Data location
- Forensic importance: “Every file leaves a trace in MFT”



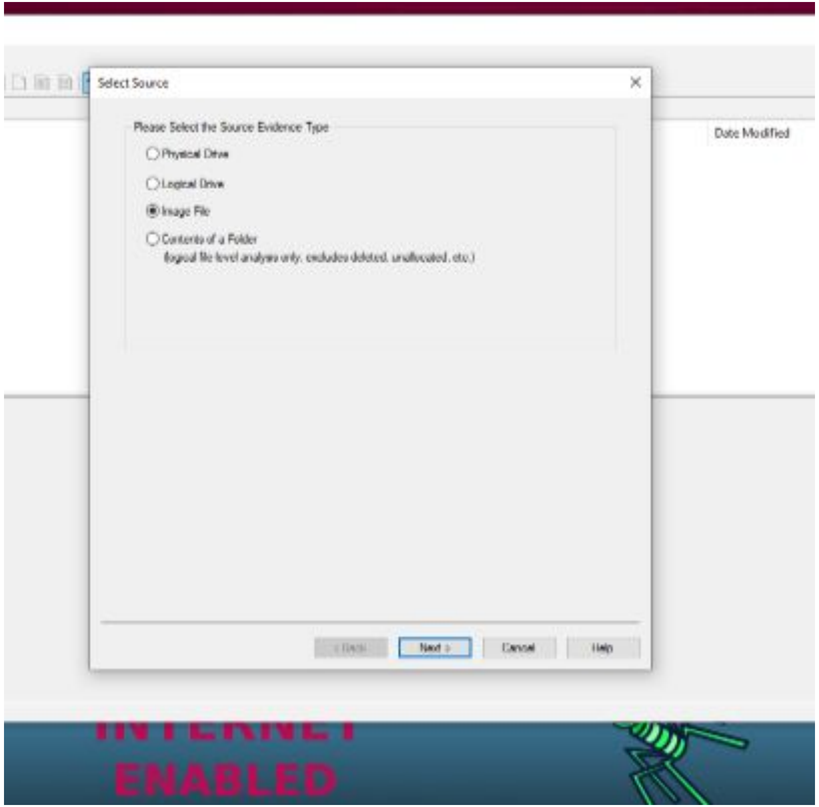
Introducing FTK Imager



To start analyze disk forensic artifacts:

Types of disk image:
- raw (.dd)
- E01 (EnCase)
- AFF (Advanced Forensic Format)

Introducing FTK Imager



Select Source

Please Select the Source Evidence Type

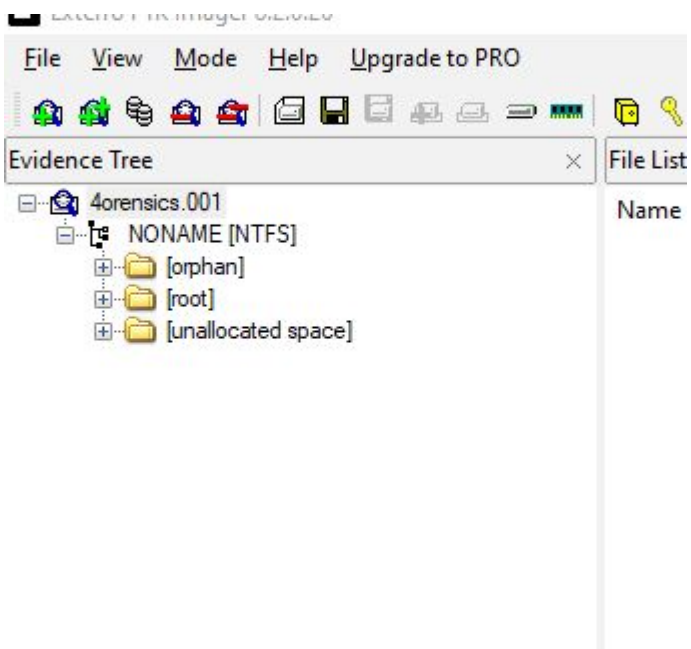
○ Physical Drive

○ Logical Drive

● Image File

○ Contents of a Folder
(logical file level analysis only; excludes deleted, unallocated, etc.)

Evidence Tree Explained



NONAME [NTFS]

- The file system detected inside the image.
- “NTFS” shows this is a **Windows NT File System**.

[root]

- Represents the main directory of the disk (like *C:*).
- Browse here to view normal folders and files.

[orphan]

- Contains files or directories **not linked** to any active folder.
- Often includes **deleted or corrupted entries** that still exist in the MFT.
- Forensic value: Can reveal deleted evidence or hidden activity.

[unallocated space]

- Shows areas of the disk **not assigned** to any file.
- Can still contain **residual data**, like remnants of deleted files.
- This is where forensic tools can **carve** files from raw data.

Windows File Paths Explained

C:\Users\John\Documents\Project\report.docx

Path Components Breakdown

1. C:
   - Identifies the physical or logical drive
   - C: (system), D: (secondary), E: (USB/CD)

2. \:
   - Divides directory levels (Windows uses \, Unix uses /)
   - Separates folders in the hierarchy

3. Users:
   - First folder level after drive root
   - Users, Windows, Program files

Task

1. What is the username of the device's owner
2. What web browser applications does the owner used
3. What antivirus software is installed
4. What are the files have been permanently removed from the system