# Disk Forensics

Disk Forensics is the specialized field dedicated to the analysis of disk images and their underlying file systems. The primary objective is to understand the structure of logical partitions on a storage medium and to extract and analyze digital artifacts.

The most common approach is Post-Morten Acquisition, which involves the analysis of a disk image created from a drive that has been disconnected from its original system. This practice is crucial for preserving the integrity of the evidence. In specific circumstances, however, duplicate drives - often referred to as clones or mirror copies - can be directly analyzed, negating the immediate need for a separate forensic image file.

## 1.1 Devices

**Mechanical Hard Disks (HDD).** A Mechanical Hard Disk Drive stores data magnetically on rotating circular disks called platters.

- *Physical Structure*: Platters are coated in magnetic material and are spun by a spindle motor. Common rotational speeds range from 5400 to 7200 RPM, though high-performance drives can reach speeds up to 15000 RPM. Data is organized on the platter surface into concentric circles called tracks, which are further subdivided into sectors (the smallest physical storage unit). A set of identically positioned tracks across all platters constitutes a cylinder. Mechanical arms feature read/write heads that move across the platters to execute I/O operations. A controller chip manages the interface between the drive and the host system commands.
- *Forensic Relevance*: When a file is logically "deleted", the operating system simply marks the space as available; the data remains physically on the disk until it is actively overwritten. Data may be fragmented, meaning it can be distributed across multiple non-contiguous sectors. HDDs support Self-Monitoring, Analysis, and Reporting Technology functionality, which provides a relatively reliable prediction of disk health and potential failure.

**Solid State Drives (SSD).** A Solid State Drive uses flash NAND memory to store data and, crucially, contains no moving parts.

- *Physical Structure*: Data is stored electronically in memory cells, with each cell capable of storing one or more bits of data. These cells are grouped into larger units called pages (the minimum unit for reading) and thousands of pages are grouped into blocks (the minimum unit for writing/erasing). An integrated flash controller manages all read/write and maintenance operations. Many SSDs also utilize DRAM caches to significantly reduce data access times.
- *Forensic Challenges*: Flash memory cells have a finite endurance, meaning they can only be reliably read from and written to for a limited number of cycles (typically specified in Terabytes Written). The controller employs sophisticated wear-leveling algorithms to distribute write operations evenly across the NAND cells. This process can be dynamic (writing new data to the least-used blocks) and static (periodically relocating old, static data to less-worn cells). To maintain performance and endurance, the controller uses a Garbage

Collector to permanently and securely erase invalid data from cells. The TRIM command is a special feature that an operating system sends to the SSD controller when files are deleted, prompting the controller to immediately and permanently erase the associated data blocks, thereby greatly complicating data recovery efforts. While SSDs support S.M.A.R.T., the predictive accuracy for failures is often less reliable than for HDDs due to the nature of flash memory wear.

## 1.2 Disk Acquisition and Analysis

Disk acquisition is the critical process of creating a forensically sound copy of a storage medium. Analysis then involves examining that copy to extract evidence.

**Disk Imaging Tools.** The physical analysis of a drive requires creating a bit-for-bit duplicate, or disk image. Different operating systems offer various tools for this purpose:

- *Windows*: Analysts commonly utilize specialized commercial tools such as FTK Imager or Magnet Acquire for reliable and validated image creation.
- *Linux*: The standard utility is the `dd` command. For forensic purposes, specialized variants are preferred: `dcfldd` (which includes hashing and verification on the fly) and `ddrescue` (optimized for handling drives with bad sectors) ensure greater integrity and reliability.

**Mounting and Access.** Mounting is the procedure that makes the file system within a forensic disk image or a physical drive accessible for examination by the operating system. This is done provided the source image maintains sufficient integrity. System administrators and forensic examiners use various commands and tools depending on the operating environment. On a Linux system, the standard command-line utility used for this purpose is `mount` . In Windows, utilities like Diskpart can be employed. Modern Windows systems also rely on PowerShell cmdlets such as `Get-Disk` and `Get-Partition` to manage and assign access to the file system of the mounted image.

**Partition Structure and Types.** Partitions define the logical organization of data embedded within a storage device, dictating how the operating system manages and accesses files. A drive typically contains different types of partitions serving distinct roles. A Primary Partition is the main area where the Operating System is usually installed and is generally configured to be bootable. The System Partition holds the essential files required to boot the Operating System itself, such as the bootloader. Finally, a Recovery Partition is a dedicated area containing tools and system images used to restore the operating system to a previous or factory state.

The overall organization of these partitions is defined by one of two main Partitioning Schemes. The older scheme, Master Boot Record (MBR), is limited in its capacity, supporting only four primary partitions and a maximum logical drive size of 2 TB. The modern standard is the GUID Partition Table (GPT). This scheme offers significantly expanded capabilities, supporting up to 128 primary partitions and logical drive sizes well beyond 2 TB. GPT is the standard partitioning method compatible with Unified Extensible Firmware Interface (UEFI) systems, which have largely replaced the older BIOS firmware interface.

### File Systems in Windows

A file system represents the methodology an Operating System uses to manage, store, organize, retrieve, and manipulate files on a storage device. Partitions are formatted with a specific file system to enable this structure.

- *FAT and exFAT*: FAT (File Allocation Table) and exFAT (Extended File Allocation Table) are simpler, older file systems. They organize data into clusters, which are the fundamental units for storing files. Essential bootstrap information is contained within a boot sector at the start of the file system. Standard FAT systems have a maximum file size of 4 GB and a maximum volume size of 8 TB, although Windows commonly imposes a 32 GB limit for formatting. exFAT extends these limits to support larger drives, making it suitable for flash drives and external media.
- *NTFS (New Technology File System)*: NTFS is the modern, robust, and feature-rich file system primarily used by Windows. Its central core is the Master File Table (MFT), which functions as a database containing records for every filename, attribute, and piece of metadata within the logical volume. A key concept in NTFS is that everything is treated as a file, including the MFT itself. NTFS supports several advanced features critical for data integrity and security, including encryption and journaling. The journaling feature involves a special file, the `LogFile` , which records every change performed to files before they are fully written, enabling crash recovery. NTFS supports a massive maximum file size of 16 exabytes and a maximum volume size of 256 TB.

Slack space is residual, unused data storage area created due to the way operating systems allocate space. Data is typically written in clusters (or blocks), often in multiples of 4 KB. When a file's size is not an exact multiple of the cluster size, the remaining portion of the cluster is not used by that file. This unused space is the slack space, and it may still contain fragments of data from previously stored, deleted files, making it a valuable source of forensic artifacts.

**NTFS Forensics: Master File Table (MFT).** The MFT is a specialized, hidden system file ($MFT) located in the root directory of an NTFS volume. It is composed of sequential MFT records, where the first sixteen are reserved for special system files:

**(1)** `$ MFTMirr` : Contains a partial backup of the initial MFT records for redundancy.

**(2)** `$ LogFile` : The critical partition journal file that aids in crash recovery.

**(3)** `$ Volume` : Contains vital volume information such as the label, identifier, and version.

**(4)** `$ AttrDef` : Holds the definitions for all standard MFT attributes.

**(5)** `.` : This record represents the base directory of the entire volume, serving as the starting point for the file system hierarchy.

**(6)** `$ Bitmap` : A structure that contains the allocation status (used or free) for all clusters on the volume.

**(7)** `$ Boot` : Contains the boot record of the volume.

**(8)** `$ BadClus` : Marks clusters that have been identified as unusable or "bad".

**(9)** `$ Secure` : Stores information about security descriptors and access control lists.

**(10)** `$ UpCase` : This file contains a crucial lookup table that stores all Unicode characters in uppercase. The NTFS file system uses this table to perform case-insensitive comparison for filenames, which is essential for maintaining compatibility and consistency across the Windows operating environment.

**(11)** `$ Extend` : This is a special directory that contains important sub-entries, including the `UsnJournal` (Update Sequence Number Journal), which specifically tracks all changes to files and folders on the volume.

**(12)** *Reserved*: These MFT records are marked as reserved but are typically kept empty. This is a design strategy by Microsoft to allow for future expansion and new features within the NTFS architecture without requiring a complete file system overhaul.

Once the initial set of reserved system records is accounted for, the remaining entries in the MFT are allocated to track all user files and directories on the volume. When a user file is created, it is assigned the next available MFT record number. If a file is later deleted, its MFT record is simply marked as free, but the record itself, along with its metadata, is not deleted. This preserved metadata is the foundation for file and artifact recovery in digital forensics.

Each MFT record is typically 1024 bytes long and is organized into a sequence of attributes. These attributes contain all the necessary metadata about a file or directory. An MFT record begins with a fixed header and includes several mandatory attributes:

- *Header (Offset 0x00)*: The record always starts with the FILE signature from offsets 0x00 to 0x03. This signature confirms that the entry is a valid MFT record.
- *STANDARD_INFORMATION Attribute (Offset 0x50)*: This attribute holds essential file system metadata, most notably the timestamps and file permissions. These timestamps follow the MACB standard (Modified, Accessed, Changed, Birth/Creation). The time values are measured in 100 nanosecond intervals since January 1, 1601, 00:00:00 UTC.
- *FILE_NAME Attribute (Offset 0xF0)*: This attribute stores the name of the file or directory. Note that a file can have multiple `$ FILE_NAME` attributes.
- *DATA Attribute*: Following the file name, the actual data content of the file is stored. For small files, the data may be contained directly within this attribute within the MFT record. For larger files, the attribute holds pointers to the clusters where the data is stored on the volume.

**NTFS Forensics: Bitmaps.** The Bitmap file is a critical system file that maintains the allocation status of the entire volume. This file contains a continuous sequence of bits, where each individual bit corresponds to a specific cluster on the disk. If a cluster is allocated, its corresponding bit in the `$ Bitmap` file is set to `1` .

**NTFS Forensics: Journaling Files.** NTFS utilizes two separate journaling files, the `$ LogFile` and the `UsnJournal` , each serving a distinct purpose in system reliability and forensics.

- *LogFile*: Contains a precise, transactional record of every low-level action performed by the file system (e.g., allocating a cluster, updating an MFT attribute) before it commits the change. Tools like LogFileParses can analyze its content.

- *UsnJournal*: Focuses exclusively on tracking user-level changes to files and folders, such as creation, modification, deletion, and renaming. It is a simplified, high-level history designed for applications like backup software.

The `UsnJournal`, contained within the `$ Extend` MFT entry, is a high-level change tracking mechanism. It focuses specifically on which files/folders were changed and how they were changed, rather than the raw file system transactions. Its primary function is to support incremental backups and applications that need a lightweight history of user-driven modifications. For forensics, both files are crucial, but the `LogFile` provides deeper, more granular evidence of file system activity.