Digital Forensics

Federico Conti - 4991779

2024/25

Contents

Forensic Acquisition

Acquisition is the process of cloning or copying digital data evidence.

- forensically sound (integrity and non-repudiation)
  - the copies must be identical to the original
  - the procedures must be documented and implemented using known methods and technologies, so that they can be verified by the opposite party
- a critical step
  - proper handling of data ensures that all actions taken on it can be checked, repeated, and verified at any time
  - incomplete or incorrect handling of data has the potential to compromise the entire investigation

It is generally recommended to avoid conducting analysis on the original device (namely, best evidence).

Creating a forensic image is typically considered the most effective method for preserving digital evidence (One or more, usually two).

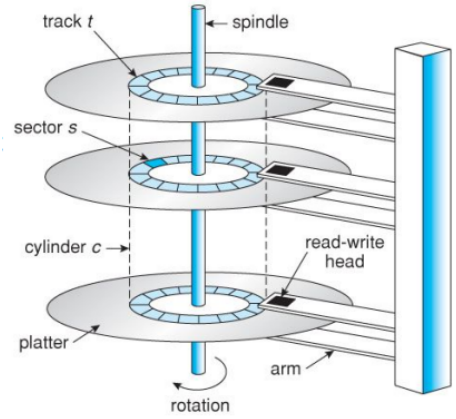
Accessing the original media only once during the acquisition phase can help minimize the risk of altering or damaging the evidence

HDD and SSD technologies

HDD

A **hard disk** is a sealed unit containing a number of platters in a stack:

- each platter has two wothey moverking surfaces
- each working surface is divided into a number of concentric rings called tracks
  - the collection of all tracks that are the same distance from the edge of the platter is called a cylinder.
- each track is further divided into sectors
  - a sector is the smallest unit that can be accessed on a storage device
  - traditionally containing 512 bytes of data each, but recent hard drives have switched to 4KB sectors (Advanced Format)
  - a cluster is a group of sectors (from 1 to 64 sectors) that make up the smallest unit of disk allocation for a file within a file system



The data on a hard drive is read by read-write hands. The standard configuration uses one head per surface and they moves simultaneously from one cylinder to another.

A **low level format** is performed on the blank platters to create data structures for tracks and sectors

- creates all of the headers and trailers marking the beginning and ends of each sector
- header and trailer also keep the linear sector numbers (cf. LBA later), and error-correcting codes (ECC)

All disks are shipped with a few bad sectors (additional ones can be expected to go bad slowly over time).

- disks keep spare sectors to replace bad ones
- ECC calculation is performed with every disk read or write: if an error is detected but the data is recoverable, then a *soft error* has occurred if the data on a bad sector cannot be recovered, then a *hard error* has occurred. A bad sector can be replace with a spare one (but any information written is usually lost)

Older hard drives used a system called **CHS (Cylinder-Head-Sector)** addressing to locate data on the disk. This method relied on:

- Cylinders (C) → The track number (a ring of data on a disk platter).
- Heads (H) → The read/write head that accesses a platter's surface.
- Sectors (S) → The smallest unit of storage on a track.

Eample: CHS (100, 2, 30) would mean: Cylinder 100; Head 2 (indicating the second platter side); Sector 30 (the exact location on that track).

CHS had physical limitations → It could only handle disks up to 504 MB (later ECHS extended this to 8 GB).

Instead of using three values (CHS), **Logical Block Addressing(LBA)** assigns a single number to each sector. LBA starts at 0 and counts up sequentially. The operating system and file system treat the disk as a continuous array of sectors, making it easier to manage.

Example: LBA 123456: The 123,456th sector on the disk.

SSD

A **Solid-State Drive (SSD)** is a non-volatile storage device, meaning it retains data even when the power is off. Unlike Hard Disk Drives (HDDs), which use spinning magnetic platters, SSDs rely on flash memory chips to store data.

- The smallest unit of an SSD is a page, which is composed of several memory cells: the page sizes are 2KB, 4KB, 8KB, 16KB or larger (usually they are 4 KB in size).
- Several pages on the SSD are summarized to a block: the block size typically varies between 256KB (128 pages * 2KB per page) and 4MB (256 pages * 16KB per page)

Operation	Description
Read and Write	An SSD can read and write data at the page level.
Write	Writing is only possible if other pages in the block are empty. Otherwise, it leads to write amplification.
Erase Data	An SSD can only erase an entire block at once due to the physical and electrical characteristics of the memory cells.

Modifying data requires a **Program/Erase (P/E) cycle**.

- During a P/E cycle, an entire block containing the targeted pages is written to memory
- The block is then marked for deletion, and the updated data is rewritten to another block

The erase operation does not happen immediately after data is marked for deletion. Instead, the SSD performs it asynchronously when necessary to optimize performance.

Garbage Collection helps free up space efficiently while minimizing interruptions to read/write operations.

Every flash memory cell has a limited number of P/E cycles before it wears out Wear leveling is a technique used by SSDs to distribute writes evenly across all memory blocks.

Unlike HDDs, SSDs cannot simply overwrite deleted files. If deleted data is not managed properly, unnecessary data copies can cause write amplification, increasing wear on the SSD. TRIM command allows the OS to inform the SSD which pages are no longer needed, enabling it to manage space more efficiently.

Forensic Investigators Face a Big Problem with SSDs|

TRIM permanently deletes data by triggering the garbage collector, making data recovery impossible. The garbage collector operates independently within the SSD controller, meaning:

- Even a hardware write blocker (a forensic tool to prevent data changes) cannot stop it.
- Data can change midway or between acquisitions, complicating forensic investig

Interface standards and protocols

Disks are accessed using standard interfaces that define how they physically and logically connect to a computer system. Each standard improves data transfer speeds and fixes limitations from older technologies. A disk interface consists of two key components:

- Physical Connection → Defines the type of cable and connector used to attach the disk to the system.
- Logical Connection → Defines the protocol that controls how data is transferred between the disk and the computer.

ATA (Advanced Technology Attachment):

a widely used interface standard with multiple versions:

- ATA-1, ATA-2, . . . , ATA-8 → Each new version improves speed and capacity.
- ATAPI (ATA Packet Interface) → Allows removable media (CD/DVD drives) to be connected using ATA but still uses SCSI commands for data transfer.

Type	Description
PATA (Parallel ATA)	Older, also known as IDE (Integrated Drive Electronics). Uses ribbon cables with multiple pins.
SATA (Serial ATA)	Modern standard introduced in ATA/ATAPI-7. Uses thin serial cables, improving speed and efficiency.
SATA 3.0	Supports speeds up to 6 Gbit/s (SATA-600). Common in modern HDDs and SSDs.
ATA-8	Introduced optimizations for SSDs, including TRIM support.

SCSI (Small Computer System Interface):

now replaced by SAS (Serial Attached SCSI) that is based on the SCSI standard, but uses a serial interface to connect storage. Better scalable and faster (supports data transfer rates of up to 24 Gbit/s).

NVMe (Non-Volatile Memory Express):

Uses a PCIe interface to connect storage devices to a computer. Commonly used for high-performance solid-state drives since it supports data transfer rates of up to 32 GB/s.

USB (Universal Serial Bus):

- uses a serial interface to connect storage devices to a computer
- mass storage is the standard protocol used for storage devices
- commonly used for external hard drives, flash drives, and other portable storage devices
- USB 3.1 Gen 1 standard supports speeds up to 5 Gbit/s, while the USB 3.1 Gen 2 standard, supports speeds up to 20 Gbit/s.

ATA specification

Introduced in ATA-3, **hard disk passwords** are an optional security feature designed to restrict unauthorized access to a hard drive. However, it is a lock mechanism, not encryption, meaning data remains unencrypted and could be accessed by other means.

There are two passwords:

1. User Password → Set by the owner.
2. Master Password → was designed so an administrator can gain access in case the user password was lost (every hard disk is initially supplied with an undocumented master password).

If passwords are being used, there are two modes that the disk can operate:

1. high security mode: the user and master password can unlock the disk
2. maximum-security mode: the user password can unlock the disk but the master password can unlock the disk after the disk content have been wiped

A protected HD will require the `SECURITY_UNLOCK` command to be executed with the correct password before any other ATA command. After the password has been entered, the disk works normally until the disk is powered on

Some ATA commands are still enabled on the HD when it is locked (so it may show as a valid disk when it is connected to a computer); however, trying to read data from a locked disk will produce an error

Setting the Password:

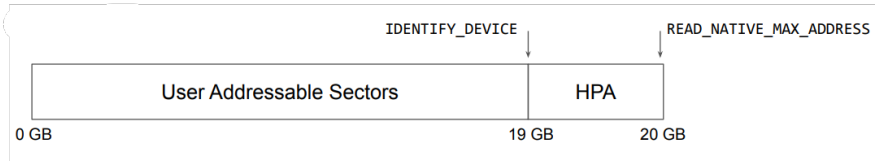
- Can be configured via BIOS settings.
- Linux users can manage HDD passwords using tools like hdparm.

Introduced in ATA-4, the **Host Protected Area (HPA)** is a hidden storage section on a hard disk that is not accessible to the operating system. It is used mainly by hardware vendors for system recovery files, diagnostics, or factory reset tools. A HPA is at the end of the disk and when used, it can be accessed by reconfiguring the hard disk.

Two ATA commands that return maximum physical addressable sectors

- `READ_NATIVE_MAX_ADDRESS`: return the maximum physical address
- `IDENTIFY_DEVICE`: return only the number of sectors that a user can access

To create an HPA, the `SET_MAX_ADRESS` command is used to set the maximum address to which the user should have access (to remove it, use `SET_MAX_ADDRESS = READ_NATIVE_MAX_ADDRESS`).



the `SET_MAX_ADRESS` command support different settings, e.g.,

- volatility bit: the HPA exist after the hard disk is reset or power cycled (otherwise the effect is permanent)
- locking command: prevents modification to the maximum address until next reset

when the BIOS requires to read/write some data in the HPA it uses `SET_MAX_ADRESS` with volatility bit and locking.

It is possible to protect settings with a password (different from HD passwords).

The **Device Configuration Overlay (DCO)** was introduced in ATA-6 and allows manufacturers to limit the apparent capabilities of a hard disk. This feature enables backward compatibility with older systems but can also be exploited to hide data.

A computer uses the `IDENTIFY_DEVICE` command to check an HDD's specifications (size, features, supported commands). If a DCO is applied, the `IDENTIFY_DEVICE` command will not show the actual full disk size or features.

This is achieved using two special ATA commands:

- `DEVICE_CONFIGURATION_SET` → Modifies the DCO settings to restrict visible disk space or disable features.
- `DEVICE_CONFIGURATION_RESET` → Restores the original settings, removing the DCO restrictions.

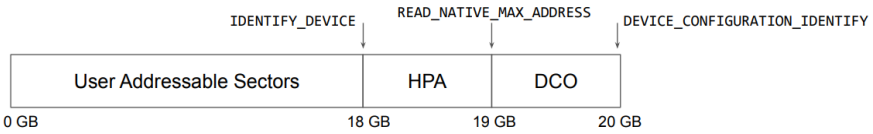
*Example:

A 2 TB hard drive can be made to appear as a 500 GB drive, hiding the remaining 1.5 TB from the operating system.*

The DCO and HPA can co-exist on the same HDD (but DCO must be set first).

The `DEVICE_CONFIGURATION_IDENTIFY` command return the actual features and size of a disk:

- we can detect DCO if `DEVICE_CONFIGURATION_IDENTIFY` $\neq$ `IDENTIFY_DEVICE`



At least three different methods for detecting HPA on Linux: `dmesg`, `hdparm`, and `disk_stat` (https://wiki.sleuthkit.org/index.php?title=Disk_stat)

Disk encryption: Bitlocker

BitLocker is a full-disk encryption feature in Windows that protects data using a multi-layered encryption system.

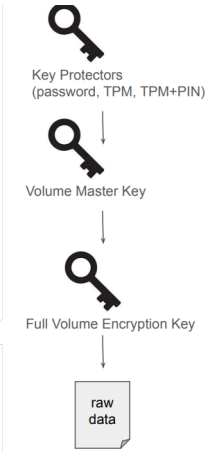
It makes use of symmetric encryption (by default, AES-128).

On modern systems, it is coupled with a Trusted Platform Module (TPM):

- the main functions of TPM are the generation, storage and secure management of cryptographic keys
- on a computer without TPM a password can be used (then BitLocker encryption will be just as secure as the password you set)

Bitlocker uses different symmetric key:

1. row data is encrypted with the Full Volume Encryption Key (FVEK)
2. FVEK is then encrypted with the Volume Master Key (VMK)
3. VMK is in turn encrypted by one of several possible methods depending on the chosen authentication type (that is, key protectors or TPM) and recovery scenarios



The use of intermediate key (VMK between FVEK and any key protectors) allows changing the keys without the need to re-encrypt the raw data in a case a given key protector is compromised or changed.

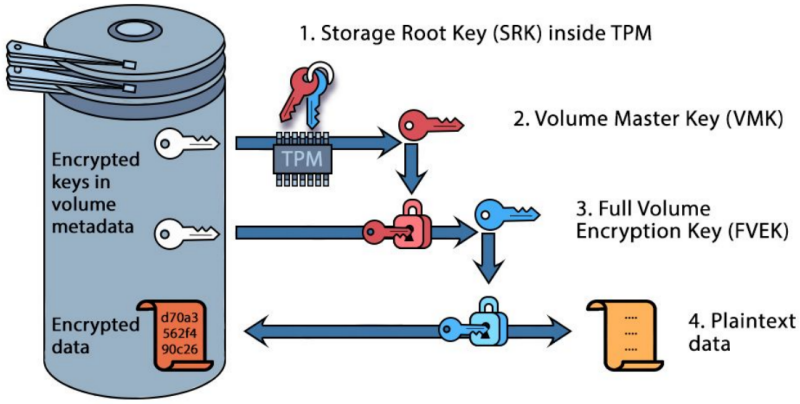
- When changing a key protector, a new VMK will be created and used to encrypt the old FVEK with the new VMK

BitLocker supports multiple key protector options, depending on the security needs and device type.

TPM only

- The TPM module (a hardware security chip) decrypts the VMK using a Storage Root Key (SRK) stored in the TPM.
- The SRK is only released if Secure Boot passes, ensuring the device boots with its original OS and configuration.
- The BitLocker volume is unlocked automatically during boot, before the user logs in.

View article.



TPM + PIN

- The TPM module will only release the VMK if the user enters a correct PIN during the pre-boot phase.
- If too many incorrect PIN attempts occur, the TPM will lock access to the encryption key, preventing brute-force attacks.

Key Takeaways:

- BitLocker is excellent for protecting against physical threats like device theft or unauthorized hard drive access.
- It does NOT protect against malware, ransomware, or unauthorized logins by users on the same computer.
- TPM + PIN is the most secure option to prevent unauthorized access, even if a device is stolen.

BitLocker poses a problem for forensic investigators, as all information on the drive will be encrypted, and therefore unreadable. Some methods for breaking BitLocker password are:

- the RAM dump/hibernation file/page file attack: this attack is universal, and works regardless of the type of protector. It dumps from the computer's volatile memory (and possibly in the page/hibernation file) the VMK that is loaded unencrypted while the volume is mounted
- BitLocker recovery keys: in many situations recovery keys are be stored in the user's Microsoft Account. Extracting those keys from their account allows instantly mounting or decrypting protected volumes regardless of the type of protector

Toolset and examples

A **loop** device is a special kind of block device that does not map to a physical hardware device (such as a hard disk) but instead maps to a regular file stored within a filesystem.

- useful to access a forensic image
- read/only can be forced
- the offset parameter could be useful to directly access a volume
- (can be used to simulate a block device to be acquired)

Key losetup Commands:

- `losetup -a`→ Shows the status of all loop devices.
- `losetup -d [device]` → Detaches a loop device.
- `losetup -f` → Finds the first available (unused) loop device.
- `losetup -o [offset]` → Starts reading data at a specific offset in the file.
- `losetup -r /dev/loop0 [srcfile]` → Sets up a read-only loop device.

dd is the precursor of all acquisition tools, allowing for the acquisition of data bit by bit in raw format.

Key `dd` Options:

- `if=` → Input file (or device to copy from).
- `of=` → Output file (or device to write to).
- `bs=` → Block size (how much data to read/write at a time).
- `conv=` → Specifies conversion options (e.g., noerror to continue on errors).

Example

```
dd if=/dev/sda of=/mnt/dest/image.dd bs=512
```

losetup and dd

In this exercise, we will simulate a block device using a compressed forensic image and interact with it as if it were a real disk.

```
wget https://github.com/enricorusso/DF_Exs/raw/main/acquisition/image.dd.gz
gunzip image.dd.gz

# Before setting up the loop device, find an available one using
lsblk
losetup -f

sudo losetup -r /dev/loop1 image.dd # Now, set up the image as a read-only loop device

sudo dmesg | tail # To verify that the loop device was correctly attached, check system logs
[84058.342422] loop1: detected capacity change from 0 to 2033664

sudo fdisk -l /dev/loop1 # To inspect the loop device and view partition details

# Since the loop device represents an entire disk,
# Linux does not automatically recognize partitions.
# Use partx to make them available
sudo partx -a /dev/loop1

mkdir -p /mnt/forensic_image
sudo mount -o ro /dev/loop1p1 /mnt/forensic_image

ls -l /mnt/forensic_image

#clean
sudo umount /mnt/forensic_image
sudo losetup -d /dev/loop1
```

In digital forensics, verifying the integrity of a forensic image is crucial to ensure that the data remains unchanged during analysis. This is done by calculating cryptographic hash values (MD5 and SHA1) before and after mounting the image → Before using the forensic image, compute its MD5 and SHA1 hashes.

```
md5sum image.dd
446144a4af914d7e55603b6042f20db1  image.dd

sha1sum image.dd
99540f5aaa170afbab722729e980fd6dc34ff323
image.dd

md5sum /dev/loop1
446144a4af914d7e55603b6042f20db1
/dev/loop1

sha1sum /dev/loop1
99540f5aaa170afbab722729e980fd6dc34ff323
/dev/loop1
```

The dd tool does not calculate hashes during acquisition, so forensic best practices require manually computing hashes before and after imaging to ensure data integrity.

```
# Instead of separately computing hashes before and after, we can stream data from dd to tee, simultane
sudo dd if=/dev/loop1 bs=512 | tee image.dd
| hashdeep -c md5,sha1 > image.src_hash #apt install hashdeep

# dd if=/dev/loop1 bs=512 → Reads data from the loop device.
# tee image.dd → Writes data to image.dd while also passing it to the next command.
# hashdeep -c md5,sha1 → Computes MD5 and SHA1 hashes as data is written.
# > image.src_hash → Saves the computed hashes to image.src_hash.

#Finale verification hash
md5sum image.dd
```

A faulty disk

In this exercise, we simulate a faulty disk by mapping a logical block device and introducing bad sectors. We then attempt to acquire it using dd, handling errors properly to maintain forensic integrity.

1. We create a logical "faulty" device (1Kb) with the command dmsetup*
   - `8 8 error` → [starting sector; add sector] maps the next 8 sectors of 512 byte (8 to 16) of the bad_disk device to an error area. This means that any attempt to read or write to bad_disk sectors 8 to 16 will generate an error.
   - `/dev/loop1` is the origin and must be initialized with a .dd (`sudo losetup /dev/loop0 image.dd/`)

   ```
   sudo dmsetup create bad_disk << EOF
   0 8 linear /dev/loop0 0
   8 8 error
   16 2033648 linear /dev/loop0 16
   EOF
   ```

2. Scan the simulated bad sectors.

   ```
   sh sudo badblocks -b 512 -v /dev/mapper/bad_disk
   ```

3. To ensure that all reads go directly to the faulty device (and are not cached), we disable readahead. Then, check the block device size:

   ```
   sudo blockdev --setra 0 /dev/mapper/bad_disk
   sudo blockdev --getsz /dev/mapper/bad_disk
   ```

4. Now, try acquiring the faulty disk with dd

   ```
   sudo dd if=/dev/mapper/bad_disk of=bad.dd bs=512
   ```

   Problem: dd stops when it hits a bad sector, preventing a complete acquisition.

5. To log bad sectors and replace them with zeros, use `conv=sync,noerror`
   - `tee bad.dd` → Writes the output to bad.dd while streaming it to `hashdeep` for hashing.

   ```
   sudo dd if=/dev/mapper/bad_disk bs=512 conv=sync,noerror
   | tee bad.dd | hashdeep -c md5,sha1 > bad_image.src_hash
   ```

6. After acquisition, compare the hash of bad.dd to the hash calculated during acquisition in `bad_image.src_hash`

   ```
   hashdeep -c md5,sha1 bad.dd
   ```

dc3dd

An enhanced version of dd designed specifically for digital forensics. It was developed by the DoD Cyber Crime Center (DC3) and includes several critical forensic features missing in standard dd.

Example

```
sudo dc3dd if=/dev/mapper/bad_disk of=bad.dd ssz=512 log=image.log hlog=hash.log hash=md5 hash=sha1
```

Image file formats

When acquiring digital evidence, the choice of image format is crucial for integrity, compatibility, and efficiency in analysis. There are two main categories of forensic image formats.

The output from dd acquisition is a raw image * it contains only the data from the source device * all the descriptive data about the acquisition (e.g., hashes values, dates, or times) need to be saved in a separate file

An embedded image contains data from the source device and additional descriptive data (metadata).

- **Expert Witness Format (EWF)**

  Joachim Metz (Google) created the libewf project, open source (https://github.com/libyal/libewf, apt install ewf-tools). It provides a library and set of tools to manage the ewf format.

  - `ewfacquire`: reads storage media data from devices and write files to EWF files.
  - `ewfexport`: exports storage media data in EWF files to (split) RAW format or a specific version of EWF files.
  - `ewfinfo`: shows the metadata in EWF files.
  - `ewfmount`: FUSE mounts EWF files.
  - `ewfrecover`: special variant of ewfexport to create a new set of EWF files from a corrupt set.
  - `ewfverify`: verifies the storage media data in EWF files

(FUSE (Filesystem in Userspace) is a Linux kernel module that allows users to mount and manage file systems without requiring root privileges or kernel modifications.) –> alternative `:uses sudo ewfmount`

- **Advanced Forensic Format (AFF)**

  Open Source format developed by Dr. Simson L. Garfinkel

  - 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 (unlimited number)
  - Digital signatures
  - Encryption with decryption on-the-fly
  - No patents

  Still lacks wide adoption (software available at https://github.com/sshock/AFFLIBv3).

Guymager

Guymager is a graphical (Qt-based) forensic imager. It is capable of producing image files in EWF, AFF and dd format (apt install guymager).

- AFF is disabled by default (`sudo nano /etc/guymager/guymager.cfg → set AffEnabled=true → sudo systemctl restart guymager`)

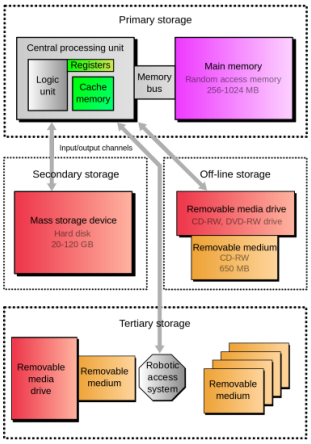
FTK Imager

FTK Imager is a data preview and imaging tool used to acquire data (evidence) in a forensically sound manner by creating copies of data without making changes to the original evidence (https://www.exterro.com/ftk-product-downloads).

File Systems

In a computer, data storage is organized in a hierarchical manner.

At the top, we have fast and directly accessible storage, such as registers and cache, while at the bottom, we have slower but larger storage, like hard drives or SSDs.



We focus on secondary (external) memory storage:

- not directly accessible by CPU –> data must be transferred to main memory (RAM) before it can be processed
- data transferred in blocks –> rather than individual bytes
- significantly slower
- non-volatile –> retains data even when power is turned off

Floppies/HDs/CDs/DVDs/BDs/SD-cards/SSDs/pendrives. . . are all block devices; following File System Forensic Analysis's terminology.

A volume is a collection of addressable blocks

- these blocks do not need to be contiguous on a physical device
- a volume can be assembled by merging smaller volumes

A partition is a contiguous part of a volume

- partitioning is optional: some removable storage does not use it

By definition, both disks and partitions are volumes. In this part of the course we deal with block-device (forensics) images, like the one acquired from actual devices.

Users don't interact directly with storage blocks—instead, they work with files and directories.

The file system creates this illusion; i.e., it handles the mapping between files/directories and a collection of blocks (usually, clusters of sectors). Consists of on-disk data structures to organize both data and metadata. There exist various file-system formats (e.g., FAT, NTFS, . . .)

(high-level) formatting a volume means to initialize those structures.

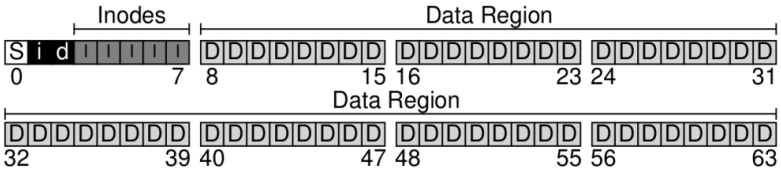
VSFS (Very Simple File-System)

In Unix-like file systems (e.g., EXT4, see `man mkfs.ext4`), each file (or other filesystem object) has an associated inode that stores its metadata. However, inode does not store file names, which are instead kept in directory structures.

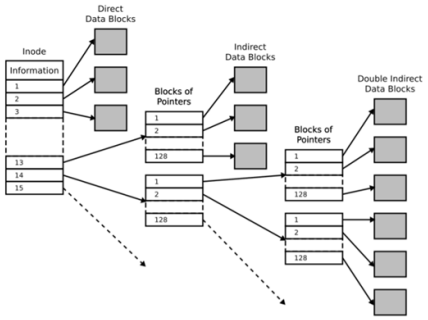
Every file system object has an inode, including:

- regular file
- directory
- symbolic link
- FIFO
- socket
- character device
- block device

Formatting means preparing: the superblock, i-node/data bitmaps, i-node table, data region.



An inode contains:

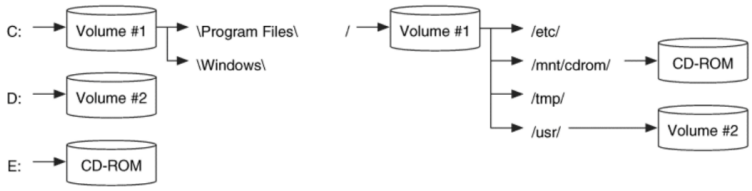


- file type
- UID/GID/permission-bits
- time information
- size in bytes
- number of hard links (AKA names)
- pointers to data blocks

To use the end-user view, a file system, stored on a **block device**, must be mounted (or "parsed")

Most modern operating systems automatically mount external storage devices when they are connected.

- In Unix/Linux there is a single root directory (/), and additional volumes are mounted within this hierarchy
- in Windows each volume (storage device/partition) is assigned a drive letter (C:, D:, E:)



Block devices can be seen as "files" themselves

- Linux special files, typically under /dev
  - various "aliases" in /dev/disk –> /by-id; /by-uuid; /bypath
  - `lsblk` lists information about available block devices

Viceversa, (image) files can be seen as block devices.

1. `losetup` command allows an image file to be treated as a virtual block device (loop device).
   - `--list`
   - `--find [--show] [--partscan] image`
   - `--detach[-all]`
2. Then, we can `mount` them.
   - Instead of manually setting up a loop device, mount can automatically create one:
   - `offset=<byte_offset>` starting point within an image file (use `fdisk -l image_file.img`)
   - `mount [-o loop] image` instead of manually setting up a loop device
   - `ro` read-only

3. Umount and check umount /dev/sda1 fsck /dev/sda1

Example

```
xz -dk two-partitions.dd.xz

# FIRST METHOD

losetup -r -o $((1*512)) /dev/loop0 two-partitions.dd  # First partition
losetup -r -o $((1026*512)) /dev/loop1 two-partitions.dd  # Second partition

# losetup -r -o $((1*512)) --find --show /tmp/two-partitions.dd
# losetup -r -o $((1026*512)) --find --show /tmp/two-partitions.dd

fdisk -l /dev/loop1 # check

mount -o ro /dev/loop0 /mnt/two-partition
mount -o ro /dev/loop1 /mnt/two-partition

# SECOND METHOD

losetup -r --find --show --partscan two-partitions.dd

mount -o ro /dev/loop0p1 /mnt/part1
mount -o ro /dev/loop0p2 /mnt/part2

umount /dev/loop0p1
umount /dev/loop0p1
```

The Sleuth Kit (TSK)

!attention: TSK always uses a term 'inode', but actually the information of filesystem is in the FAT entry directory

The Sleuth Kit (TSK) is a forensic toolkit that provides different layers of analysis for digital investigations. Each layer focuses on specific aspects of a digital storage system, allowing forensic examiners to extract and interpret data at various levels.

- `img_` for images
- `mm` (media-management) for volumes
- `fs` for file-system structures
- `j` for file-system journals
- `blk` for blocks/data-units
- `i` for inodes, the file metadata
- `f` for file names

Typically followed by:

- `stat` for general information
- `ls` for listing the content
- `cat` for dumping/extracting the content

Example

```
img_stat two-partitions.dd
img_cat two-partitions.dd

img_stat canon-sd-card.e01
```

When analyzing file systems, we categorize data into essential and non-essential based on their reliability and importance.

- Essential Data = Trustworthy & required for file retrieval.
  - If name or location were incorrect, then the content could not be read
- Non-Essential Data = Can be misleading & needs verification.
  - the last-access time or the data of a deleted file could be correct but we don't know

The Volume (or Media Management) layer in The Sleuth Kit (TSK) focuses on analyzing and managing disk partitions. This layer is crucial for identifying partition structures, extracting partitions, and verifying file system integrity.

- `mmstat image` displays the type of partition scheme
- `mmls image` displays the partition layout of a volume
- `mmcat image part_num` outputs the contents of a partition

Example

For canon-sd-card.e01

1. Find the type of partition table (mmstat)
2. List the partitions (mmls)
3. Extract the DOS FAT16 partition, by using both mmcat/dd or a dd-like tool

Check whether the SHA256 of their results match Read-only mount the FAT partition and list the files

```
mmstat canon-sd-card.e01
mmls canon-sd-card.e01

    ##OUT##
    DOS Partition Table
    Offset Sector: 0
    Units are in 512-byte sectors

         Slot      Start        End          Length       Description
    000:  Meta      0000000000   0000000000   0000000001   Primary Table (#0)
    001:  -------   0000000000   0000000050   0000000051   Unallocated
    002:  000:000   0000000051   0000060799   0000060749   DOS FAT16 (0x04)
    ###

# First method (TSK toolkit)
mmcat canon-sd-card.e01 2 > fat16_mmcat.e01

# Second method
ewfmount canon-sd-card.e01 ./rawimage/ # bit a bit copy
sudo dd if=rawimage/ewf1 of=fat16_dd.dd bs=512 skip=51
sudo umount rawimage
```

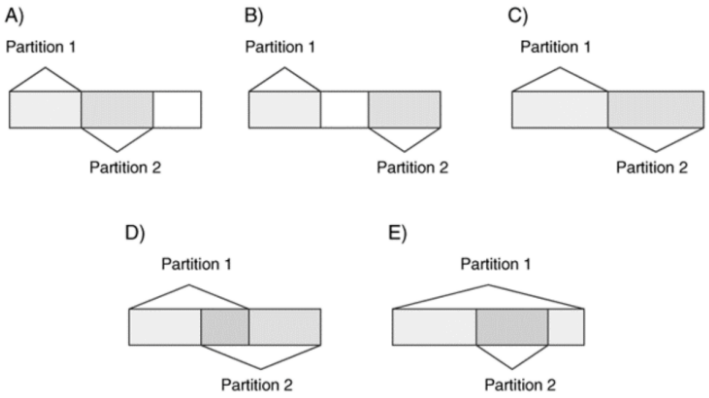
```
sha256sum  fat16_mmcat.dd fat16_dd.dd # equals


# First method (TSK toolkit)
fls -r -o 51 canon-sd-card.e01

#Second method
mount -o ro fat16_dd.dd /mnt/fat16_dd
tree /mnt/fat16_dd
```

DOS (or MBR) partition tables

The concept of MBR was introduced in 1983 with PC DOS 2.0.

It contain:

- machine code for the boot loader, which usually loads and executes the active-partition Volume Boot Record
- a 32-bit unique identifier for the disk, located at offset 440 (0x1B8).
- information on how the disk is partitioned –> four 16-byte entries (each at offset 446 (0x1BE)), allowing up to four primary partitions.
- last two bytes of the MBR contain the signature bytes: 0x55 0xAA.



1. Valid Configurations (A, B, and C):
    - These configurations ensure that partitions are either adjacent or properly aligned without overlap.
    - Partitions are defined in a way that does not create ambiguity in data storage.
2. Invalid Configurations (D and E):
    - D and E depict overlapping partitions, which is problematic.
    - Overlapping partitions may cause data corruption, boot issues, or system conflicts because two partitions would claim the same disk space.

CHS (Cylinder-Head-Sector) is the early method for addressing physical blocks on a disk.

It used a 3-byte structure:

- 10 bits for Cylinders (tracks stacked vertically)
- 8 bits for Heads (read/write heads on a disk platter)
- 6 bits for Sectors (sections of a track)

Replaced by Logical Block Addressing in ’90s.

- To convert you need to know the number of heads per cylinder, and sectors per track, as reported by the disk drive
- Yet, many tools still aligned partitions to cylinder boundaries

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	Master Boot Code															
…																
1A0																
1B0									Disk Signature						Boot ind[1]	Start head
1C0	start Sect[2]	start Cyl[2]	Sys ID[3]	End Head	End sect[2]	End Cyl[2]	Relative Sectors				Total Sectors					
1D0																
1E0																
1F0															55	AA

1. Boot indicator 0x00 = non-boot, 0x80 = bootable
2. Starting sector & starting cylinder are allocated bits, not bytes (0x1C0-0x1C1) same goes for end head and end sector

BIT	0	1	2	3	4	5	6	7	8	9	A		B	C	D	E	F
Value	Starting sector							Starting Cylinder									

3. Common partition values.

0x01	FAT12 <32MB
0x04	FAT16 <32MB
0x05	MS Extended partition using CHS
0x06	FAT16B
0x07	NTFS, HPFS, exFAT
0x0B	FAT32 CHS
0x0C	FAT32 LBA
0x0E	FAT16 LBA
0x0F	MS Extended partition LBA
0x42	Windows Dynamic volume
0x82	Linux swap
0x83	Linux

0x84	**Windows hibernation partition**
0x85	Linux extended
0x8E	Linux LVM
0xA5	FreeBSD slice
0xA6	OpenBSD slice
0xAB	Mac OS X boot
0xAF	HFS, HFS+
0xEE	MS GPT
0xEF	Intel EFI
0xFB	VMware VMFS
0xFC	VMware swap

A Master Boot Record (MBR) is typically 512 bytes and laid out like this:

```
Offset (hex) | Size | Description
--------------------------------------------
0x000        | 446  | Bootstrap code area
0x1B8        | 4    | Disk signature (sometimes called "unique MBR signature")
0x1BC        | 2    | Usually 0x0000 or may be used for copy-protection, etc.
0x1BE        | 16   | Partition entry #1
0x1CE        | 16   | Partition entry #2
0x1DE        | 16   | Partition entry #3
0x1EE        | 16   | Partition entry #4
0x1FE        | 2    | MBR signature (0x55AA)
```

Each 16-byte partition entry has the structure:

```
Byte | Description
--------------------------------------
0    | Boot indicator (0x80 = bootable; 0x00 = non-bootable)
1-3  | Starting CHS (Head-Sector-Cylinder) - often unused in modern disks
4    | Partition type (ID)
5-7  | Ending CHS (Head-Sector-Cylinder)
8-11 | Relative sectors (start in LBA)
12-15| Total sectors in this partition
```

Example

Use ImHex, writing proper patterns, to extract disk and partition information from mbr{1,2,3}.dd. Then, answer the following questions:

1. What are the three disk signatures?

2. Is there any MBR with inconsistent partitioning?
3. Are there MBRs without bootable partitions?
4. What is the largest FAT (id=4) partition?
5. Are CHS information always present?

(fdisk -l mbr2.dd)

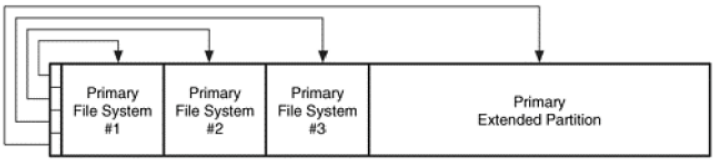
```
tar -tJf MBR123_and_GPT.tar.xz
tar -xJvf MBR123_and_GPT.tar.xz mbr1.dd

xxd -s 0x1B8 -l 4 mbr1.dd
```

Pattern editor

```
// fdisck give a same informations

#include <std/mem.pat>
struct PartitionEntry {
  u8  bootIndicator;
  u8  startCHS[3];
  u8  partitionType;
  u8 endCHS[3];
  u32 relativeSectors;
  u32 totalSectors;
};

struct MBR {
  u8 bootCode[0x1B8];       // 446 bytes
  u32 diskSignature;        // offset 0x1B8
  u16 reserved;             // offset 0x1BC (often 0x0000)
  PartitionEntry partitions[4];  // 4 partition entries, each 16 bytes
  u16 signature;            // offset 0x1FE, should be 0x55AA
};

 MBR seg[while(!std::mem::eof())] @ 0x00;
```

Extended partitions

MBR has only 4 slots for primary partitions.



To work around this limitation, one slot can be used for the primary extended partition, a partition containing other partitions.

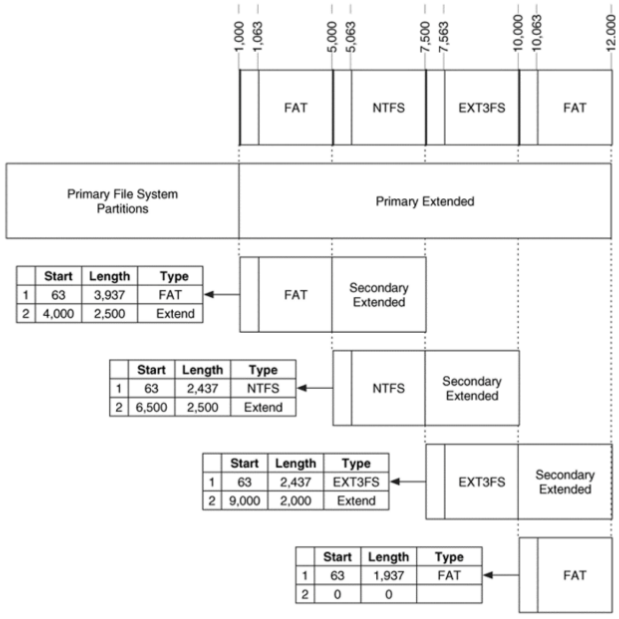
Beware of logical-partition addressing, which uses the distance from the beginning of a partition (vs the physical-addressing, from the beginning of the whole disk).

Inside the primary extended partition we find secondary extended partitions, containing

- a partition table t (with the same 512-byte structure)
- a secondary file-system partition p (logical partition), which contains a FS or other data

The partition table (t) describes:

1. Location of p (logical partition) relative to t.
2. Next secondary extended partition (if any), w.r.t. the primary extended partition



Example

ext-partitions.dd (SHA256: b075ed83211…) contains three partition tables: one primary, two extended. Analyze them with ImHex, and compare the result w.r.t. fdisk/mmls Source: (https://dftt.sourceforge.net/test1/index.html)

```
mmls ext-partitions.dd
```

```
      Slot      Start        End          Length       Description
000:  Meta      0000000000   0000000000   0000000001   Primary Table (#0)
001:  -------   0000000000   0000000062   0000000063   Unallocated
002:  000:000   0000000063   0000052415   0000052353   DOS FAT16 (0x04)
003:  000:001   0000052416   0000104831   0000052416   DOS FAT16 (0x04)
004:  000:002   0000104832   0000157247   0000052416   DOS FAT16 (0x04)
005:  Meta      0000157248   0000312479   0000155232   DOS Extended (0x05) #15724*512 = address
006:  Meta      0000157248   0000157248   0000000001   Extended Table (#1)
007:  -------   0000157248   0000157310   0000000063   Unallocated
008:  001:000   0000157311   0000209663   0000052353   DOS FAT16 (0x04)
009:  -------   0000209664   0000209726   0000000063   Unallocated
010:  001:001   0000209727   0000262079   0000052353   DOS FAT16 (0x04)
011:  Meta      0000262080   0000312479   0000050400   DOS Extended (0x05)
012:  Meta      0000262080   0000262080   0000000001   Extended Table (#2)
013:  -------   0000262080   0000262142   0000000063   Unallocated
014:  002:000   0000262143   0000312479   0000050337   DOS FAT16 (0x06)
```

Example

Someone purposely damaged the partition table of hidden-truth.dd (SHA256: 5f39a8965ec…)

1. Can you (ro) mount the partitions?
2. Can you repair the broken MBR and mount the deleted partition?

hint (ROT13): Lbh pna ernfba nobhg gur ynlbhg be trg fbzr uryc jvgu fvtsvaq (sebz GFX)

3. Can you recover the password protected "secret"?

```
fdisk -l hidden-truth.dd

    ##OUT##
    Device           Boot      Start        End   Sectors  Size Id Type
    hidden-truth.dd1               2       2050      2049    1M  4 FAT16 <3
    hidden-truth.dd2      1751214177 2311246017 560031841  267G 74 unknown
    hidden-truth.dd3            3076       8191      5116  2.5M  4 FAT16 <3
    Partition table entries are not in disk order.
    ###


 dd if=hidden-truth.dd of=hid2.dd bs=512 skip=3076 count=5115
 dd if=hidden-truth.dd of=hid1.dd bs=512 skip=2 count=2048

 ls -l hidden-truth.

    ##OUT##
    -rwxrwxrwx 1 vagrant vagrant 4194304 Mar 13 19:37 hidden-truth.dd
    # echo $((4194304/512)) == 8192 sectors
    ###

# try to find a sector 1 (0 is a boot sector)
dd if=hidden-truth.dd bs=512 skip=1 count=1 | xxd -g1

    ##OUT##
    .....
    000001e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
    000001f0: 34 37 36 39 36 66 37 36 33 34 36 65 36 65 32 31  47696f76346e6e21
    # only clue ...
    ###

# try a "brute" mount
mount -o ro, offset=$((2051*512)) hidden-truth.dd /mnt/hidden-brute

    ##OUT##
    not_so_secret.zip # a zip with pass
    ###


# does the fs cover the whole prtion in the middle?
# it is true that there is some space between the first and third partition but
# we do not know if all the space in between has been used
fsstat  hidden-truth.dd -o 2051
```

```
    ##OUT##
    File System Layout (in sectors)
    Total Range: 0 - 1023 # 3075-2051 == 1024, okey seems fair
    ###

# using a hex brefore and cyberchef
47696f76346e6e21 --> Giov4nn!
```

GPT - GUID PArtition Tables

A Universally/Globally Unique IDentifier (UUID/GUID) is a 128-bit label.

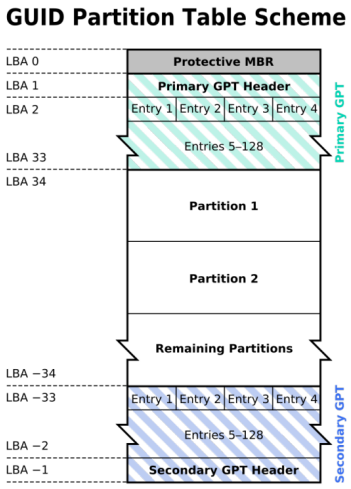
- Uniqueness: Properly generated UUIDs are statistically unique, meaning the probability of duplication is extremely low.
- Standard Format: UUIDs are typically written in a 32-character hexadecimal format divided into five groups: 8-4-4-4-12, separated by hyphens.

```
uuidgen

bdeec955-b1b8-44a2-8034-15507d431aca
```

The GPT format, used by the Extensible Firmware Interface (EFI), which replaced BIOS, is the current standard on PCs; it

- starts with a protective MBR *
- supports up to 128 partitions
- uses 64-bit LBA addresses
- keeps “mirrored” backup copies of
- important data structures

*It contains a single partition entry that marks the entire disk as being used by GPT, preventing older systems from misinterpreting the disk as unpartitioned or attempting to write to it incorrectly.



Example

Use ImHex, writing proper patterns, to extract disk and partition information from gpt.dd. Then, answer the following questions:

1. What is the disk GUID?
2. How many partitions are there?
3. What are the partition names?
4. Can you find the partition type GUIDs in the previous table?

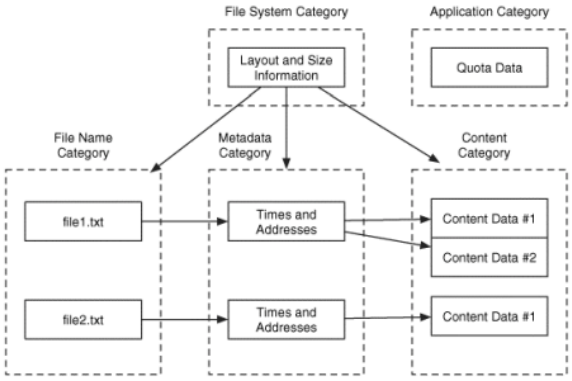
```
gdisk -l gpt.dd
mmls -t gpt gpt.dd
```

File System Analysis

A reference model for a file system based on different categories of data that are involved in file storage and management.

- File System Category: layout and size information about the entire file system, such as: file system parameters (e.g., block size, total size) the structure or mapping of data storage
- Content The actual data, stored in clusters/blocks/data-units

- MetaData: Data that describes files: size, creation date
- File Name Data that assign names to files
- Appliccation: Data not needed for reading/writing a file; e.g., user quota statistics or a FS journal



To get the general details of a file-system - `fsstat [-o sect_offs] image`

Example

1. Find the OEM Name and Volume Label (Boot Sector) in canon-sd-card.e01

```
mmls canon-sd-card.e01
```

```
    ##OUT##
        Slot      Start        End          Length       Description
    000:  Meta      0000000000   0000000000   0000000001   Primary Table (#0)
    001:  -------   0000000000   0000000050   0000000051   Unallocated
    002:  000:000   0000000051   0000060799   0000060749   DOS FAT16 (0x04)
    ###
```

```
fsstat -o 51 canon-sd-card.e01
```

2. Check whether the partition types are correctly set inside two-partitions.dd

```
mmls two-partitions.dd
```

```
    ##OUT##
        Slot      Start        End          Length       Description
    000:  Meta      0000000000   0000000000   0000000001   Primary Table (#0)
    001:  -------   0000000000   0000000000   0000000001   Unallocated
    002:  000:000   0000000001   0000001025   0000001025   DOS FAT16 (0x06) # wrong
    003:  000:001   0000001026   0000002047   0000001022   DOS FAT12 (0x01)

    ### Partition table can be modified
    ###
```

```
fsstat -o 1 two-partitions.dd # FAT12
fsstat -o 1026 two-partitions.dd # FAT12
```

Example

inside the image file two-partitions.dd

1. look for the strings

- “didattica”
- “wDeek”"
- "tool
- “secret”

```
strings two-partitions.dd | grep -E "didattica|wDeek|tool|secret" # secret,wDeek,didattica
or
strings two-partitions.dd | ag "didattica|wDeek|tool|secret"
or
xxd -g1 two-partitions.dd| grep -C 3 ecre
```

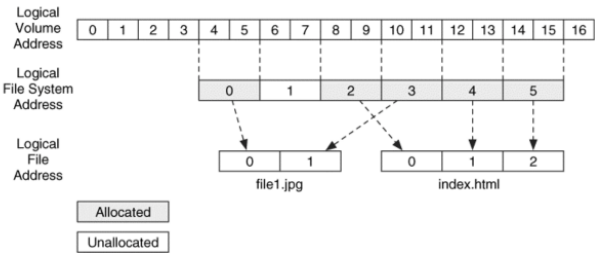
2. (ro) mount its partitions, and look for the same strings inside the contained files

```
losetup -r --find --show --partscan two-partitions.dd

mount -o ro /dev/loop0p1 /mnt/part1
mount -o ro /dev/loop0p2 /mnt/part2

grep -rE "didattica|wDeek|tool|secret" /mnt/part1 # null
grep -rE "didattica|wDeek|tool|secret" /mnt/part2 # tool
```

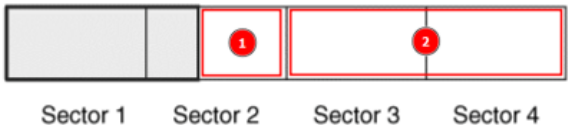
Do some string appear only in one of the two searches? Can you guess why?

Each sector can have multiple addresses, relative to the start of the…

- storage media: physical address
- volume: (logical) volume address
- FS [data area]: (logical) FS address AKA (logical) cluster number
- file: (logical) file address AKA virtual cluster numbers



When writing a 612-byte file in a file system with 2K clusters (where each sector is 512 bytes), the way data is allocated creates slack space—unused but allocated storage that may contain remnants of previous data.



When investigating deleted files, forensic analysts use two major approaches:

1. Metadata-based

   If the file is deleted but metadata still exists, we can recover:

   - File size, timestamps, and allocated sectors/clusters.
   - Orphaned files (files with no full path reference)

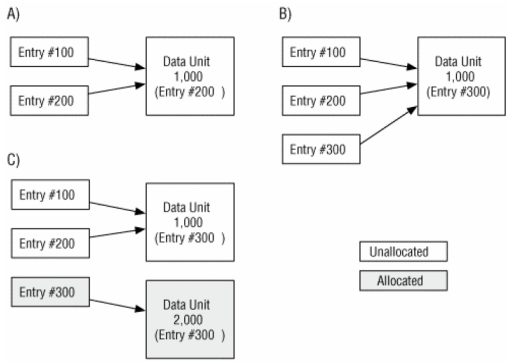
2. Application-Based

Used when metadata is unavailable:

- Typically from un-allocated space
- Does not need any FS information

Example

Where do data-units come from?



A.

- Entry#100 initially points to Data Unit 1,000.
- Entry #200 is created after #100 is deleted and reuses the same data unit.

This means that even after deletion, old data might still be recoverable unless overwritten.

C.

- Entry #300 is now assigned a completely new Data Unit (2,000).
- Entry #100 and #200 had used Data Unit 1,000, but it is now unallocated.

The original content in Data Unit 1,000 might still be present but no longer linked to any active file. (Carving).

TSK metadata commands

The Sleuth Kit (TSK) provides powerful commands to analyze file system metadata, particularly focusing on inodes, which store key file attributes.

1. `ils [-o sect_offs] image` - list inode information
    - `-r` → Lists only removed (deleted) files
    - `-a` → Lists only allocated (active) files
    - `-m` → Displays inode details in a format compatible with mactime (used for timeline analysis)
2. `istat [-o sect_offs] image inum`- dumps detailed metadata of a specific file or inode

!!! TSK uses the inode abstraction even for file systems that do not natively have them.

- Some file systems (e.g., FAT32) do not have inodes, but TSK emulates them to allow a consistent analysis approach

3. `ifind [-n filename] [-d data-unit] [-o offset] image` - viceversa, to find the inode corresponding to a data-unit or file name
    - `strings -t d disk-image.dd | grep "password"`- gives you an offset (e.g., `123456`) where the data appears.
    - `ifind -d $((123456/4096)) disk-image.dd`- $((n/block-size)) returns the inode number

4. `ffind [-o sect_offs] image inum` - lists the names using the inode (useful when names are not inside the "inode")
5. `icat [-o sect_offs] image inum` - extracts and displays the contents of a file based on its inode number.
   - `-s` → Includes slack space (unused space in the last cluster of a file)
   - `-r` → Attempts to recover deleted files

   Note: deleted content may be present in unallocated data (without metadata pointing to it). To check/dump blocks:
   - `blkstat image block` - displays metadata about a specific block (e.g., allocation status, timestamps, etc.)
   - `blkcat image block [how-many-blocks]` - outputs the raw content of a specific block
   - `blkls` - lists or outputs blocks too
6. `fls [-o sect_offs] image [inum]` - list files inside the directory corresponding to the inode number
7. `ffind [-o sect_offs] image inum` - lists the names using the inode (useful when names are not inside the "inode")

Example

Let's find out why some of the following strings appear in one search and not the other

```
mmls two-partitions.dd
```

```
##OUT##
     Slot      Start        End          Length       Description
000:  Meta      0000000000   0000000000   0000000001   Primary Table (#0)
001:  -------   0000000000   0000000000   0000000001   Unallocated
002:  000:000   0000000001   0000001025   0000001025   DOS FAT16 (0x06)
003:  000:001   0000001026   0000002047   0000001022   DOS FAT12 (0x01)
###
```

```
strings -t d two-partitions.dd | grep -E "didattica|wDeek|tool|secret"
```

```
##OUT##
20514 and I have a secret message ;)
547396 wDeek
547436 /home/gio/didattica/file-systems/vol_fs_analysis/examples/pp/test
###
```

- End of first partition = (1025*512) = 524800 –> "secret" is in the firts partition.
- Start of second partition = (1025*512) = 525312 –> "wDeek" is int the second partition.
- End of second partition = (1025*512) = 1048064 —> "didattica" is in the seconf

1. Find "secret"
   - Sector number of "secret" = (20514/512) = 40 **at begining of the disk, but partition start at sector 1**
   - Offset = (40-1) = 39

```
ifind -d 39 -o 1 two-partitions.dd # get 4 (a indo of block 39 of partition start 1)

istat -o 1 two-partitions.dd 4
```

```
##OUT##
```

```
    Directory Entry: 4
    Allocated
    File Attributes: File, Archive
    Size: 34
    Name: HELLO.TXT

    Directory Entry Times:
    Written:        2023-03-16 08:57:32 (EDT)
    Accessed:       2023-03-16 00:00:00 (EDT)
    Created:        2023-03-16 08:57:32 (EDT)

    Sectors:
    39 0 0 0 # use only one sector
    ###

icat -s -o 1 two-partitions.dd 4

    ##OUT##
    Hi there! ...
    ###

# We note that the size of ls hello is (34B) < oh the size dd rows (64)

dd if=two-partitions.dd bs=512 count=1 skip=40 | hexdump -C
ls -l hello.txt
```

2. Find “wDeek” and “didattica”
    - Sector number of “secret” = (547396/512) = 1069 **at begining of the disk, but partition start at sector 1026**
    - Offset = (1069-1026) = 43

```
ifind -d 43 -o 1026 two-partitions.dd # get 6 (a indo of block 43 of partition start 1026)

istat -o 1026 two-partitions.dd 6

    ##OUT##
    Directory Entry: 6
    Not Allocated # DELETED --> not mounted by OS
    File Attributes: File, Archive
    Size: 4096
    Name: _EST~1.SWP

    Directory Entry Times:
    Written:        2023-03-16 09:04:10 (EDT)
    Accessed:       2023-03-16 00:00:00 (EDT)
    Created:        2023-03-16 09:04:10 (EDT)

    Sectors:
    43 44 45 46 47 48 49 50
    ###

icat -o 1026 two-partitions.dd 6 | strings
```

```
    ##OUT##
    b0VIM 8.2
    root
    wDeek
    /home/gio/didattica/file-systems/vol_fs_analysis/examples/pp/test
    3210
    #"!

    ###
```

3. Find “tool”

```
fls -rp two-partitions.dd -o 1026

    ##OUT##
    r/r 4:  wikipedia.txt
    r/r * 6:        .test.swp
    r/r * 8:        test
    v/v 16083:      $MBR
    v/v 16084:      $FAT1
    v/v 16085:      $FAT2
    V/V 16086:      $OrphanFiles
    ###


istat -o 1026 two-partitions.dd 4

    ##OUT##
    Directory Entry: 4
    Allocated
    File Attributes: File, Archive
    Size: 3934
    Name: WIKIPE~1.TXT

    Directory Entry Times:
    Written:        2023-03-16 09:04:24 (EDT)
    Accessed:       2023-03-16 00:00:00 (EDT)
    Created:        2023-03-16 09:04:24 (EDT)

    Sectors:
    39 40 41 42 55 56 57 58
    # we see that the cluster is not consecutive and string "tool"
    # is fragmented in "to...ol"
    ###

icat -o 1026 two-partitions.dd 4 | strings | hexdump -C | grep -C 6 tool
```

Carving

Is a method of recovering files without relying on metadata (like file names, paths, or inodes). It works by identifying file signatures (headers & footers) and extracting the data between them.(E.g., 0xFF 0xD8 and 0xFF 0xD9 for JPEG files).

Example

Inside eighties.dd (cc121c3a037f904a4fa5ef51263df9fdb800d89af7330df22615802b81821f9d) there is a FAT file system with some deleted content. In particular, there were files with the following SHA256 hashes:

- 4410aaee5ae15917c064f80a073ec75260482b7035fad58c85f1063d0b795733
- 1b756ad00ad842c3356c093583e2e4fab2540e15ca88750606f45f7efd1f4d26
- 592f47dfcbeda344fc394987b6e02a65a35d4d849d35d2fc821e5be1889c645d
- 8a461036c70736eb4ca83e9062318c8293be2baad1c475c41c1945221559048e
- 0d176b77f6b81468eb7ba367d35bdcbd8fdfc63445c2cc83c5e27c5e0b4c1a14

Can you recover and identify them?

```
fls -rp eighties.dd or ils -r eighties.dd
    ##OUT##
    # seven deleted (*)

    r/r * 3:        _
    r/r * 4:        _
    r/r * 5:        _8.gif
    r/r * 6:        _8.txt
    v/v 523203:     $MBR
    v/v 523204:     $FAT1
    v/v 523205:     $FAT2
    V/V 523206:     $OrphanFiles
    -/r * 517:      $OrphanFiles/_live.jpg
    -/r * 518:      $OrphanFiles/_8k.jpg
    -/r * 581:      $OrphanFiles/_monty.tzx
    ###

icat eighties.dd 6 | sha256sum # ok
icat eighties.dd 5 | sha256sum # icat fail sha

icat eighties.dd 5 | xxd -g1 # magic is gif, but there is some text
icat eighties.dd 5 > fake.gif # mmm...blurred ...

# wait ... two files cannot share the same sector

istat eighties.dd 5
    ##OUT##
    Size: 2426
    Name: _8.gif
    Sectors:
    108 109 110 111 112 0 0 0
    ###

istat eighties.dd 6
    ##OUT##
    Size: 1456
    Name: _8.txt
    Sectors:
    112 113 114 0
```

```
    ###

# Two possible cases:
# 1. the file may have been overwritten (nothing can be done)
# 2. the gif was framed,
    # first it was created a txt after gif ...
    # the gif used space that was previously empty in the txt file and continued to use other space

# This information is saved in FAT, but when a file is deleted, the cluster chain is lost.
# then we can recover the first cluster and thanks the length  we can find other cluster

# cluster size is 4 sectors
fsstat eighties.dd
    ##OUT##
    Cluster Size: 2048 # 2048/512=4
    ###

img_cat -s 108 -e 111 eighties.dd > fake2.gif
img_cat -s 116 -e 119 eighties.dd >> fake2.gif # okey now its clear

sha256sum fake2.gif # but not yet, because here we have taken two clusters

# the file must be size: 2426, these bytes actually make up the .gif file
dd bs=1 count=2426 if=fake2.gif of=speriamo.gif
sha256sum speriamo.gif # OK 1b756...
```

FAQ:

- If the size of the .gif was 2426, why did I cat 2 custer (2048/512=4 sectors) 108-111/116-119 and not 2426/512 = 5 sectors ?
- **In the FAT file system, files are not saved by sectors, but by clusters.**
- why 116-119 and not 112-115?
- Because sectors 112–114 are used by another deleted file

FAT

The FAT (File Allocation Table) File System is one of the earliest and simplest file systems, first developed in 1977/1978. Over time, it evolved into three main versions: FAT12, FAT16 and FAT32.

The number indicates the # of bits used to identify clusters

- FAT12 can address 212 = 4096 clusters. Windows permits cluster sizes from 512 bytes to 8 KB, which limits FAT12 to 32 MB
- FAT16 can address 216 = 65, 536 clusters
- FAT32 can address 228 clusters (top 4 bits used for other purposes)

Actually, first 2 & last 16 are reserved: usable clusters are slightly less.

Uses the MSDOS 8.3 filename format – Only 8 characters for the name + 3-character file extension (e.g., FILE1234.TXT).

VFAT (Virtual FAT) extends FAT to support long filenames with Unicode, maintaining backward compatibility.

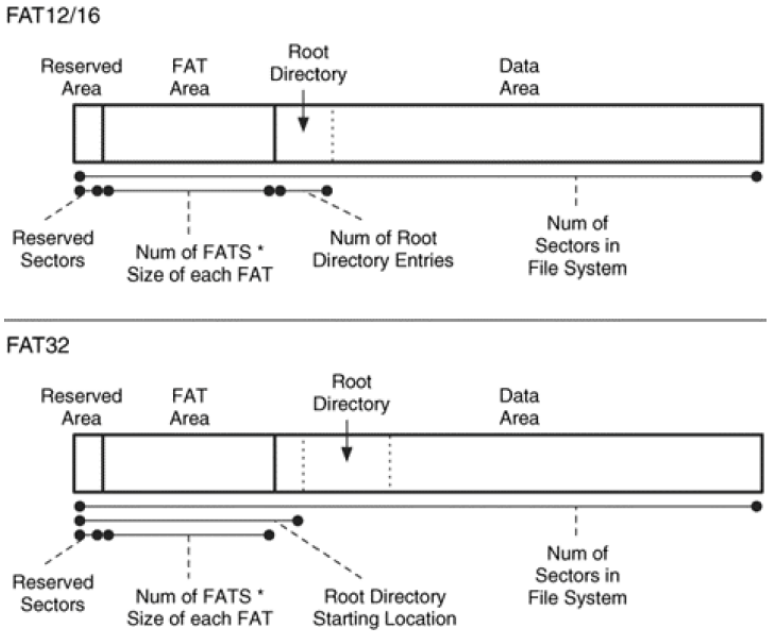
File sizes are stored as 32-bit integers, meaning the largest file size FAT32 can handle is 4 GB.

File sizes are stored as 32-bit integers.

Volume Organization

In FAT file systems, the storage device is divided into specific regions, each serving a defined role:

- The Volume Boot Record (VBR) contains the so-called BIOS Parameter Block
- The root directory of FAT12/16 has a fixed location and size
- FAT32 boot sector includes the locations of the root directory, FSINFO structure (that keeps track of free clusters, to optimize allocations), and boot-sector backup (should be 6)



1. Reserved Area

- Starts at sector 0.
- Contains the Volume Boot Record (VBR or Boot sector), which holds key information about the file system.
- FAT12/16: Usually 1 sector (only the VBR); FAT32: Larger because it includes FSINFO structure (helps track free clusters).

2. FAT Area

- follows the reserved area, and its size is calculated by multiplying the number of tables by their size

3. Data Area

- Clusters are only in Data Area, numbered from 2 (!!!) and after the root directory for FAT12/16
- Data could be also hidden after the last valid entry in a FAT table

The “Small Sectors” and “Large Sectors” fields represent the total number of sectors in the volume. Only one of these fields is used, and the other is set to zero.

Green (BIOS Parameter Block - BPB):

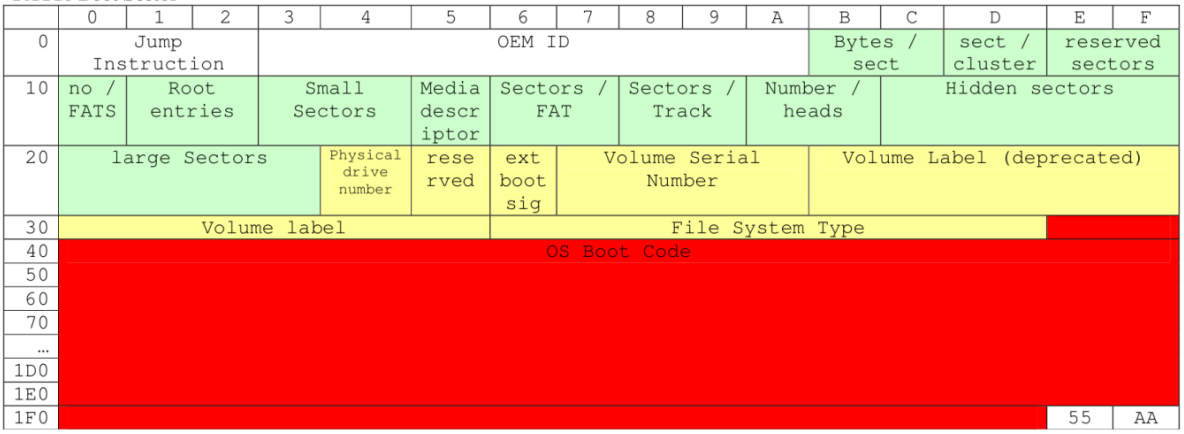
- Essential fields required for the basic operation of the file system.
- Defines sector sizes, cluster sizes, and disk structure.

Yellow (Extended BIOS Parameter Block - EBPB):

- Additional metadata introduced in later FAT versions.
- Includes details like the Volume Serial Number, Boot Signature, and Volume Label.

Boot sector FAT12/16

FAT16 Boot Sector



Boot sector FAT32

FAT32 Boot Sector

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	Jump Instruction			OEM ID								Bytes / sect		sect / cl uster	reserved sectors	
10	no / FATS	0x0000		0x0000		Media descr iptor	0x0000		Sectors / Track		Number / heads	Hidden sectors				
20	large Sectors Total sectors in volume						Sectors / FAT		0x0000		File System Version	Root(first) Cluster Number				
30	FS Info sector		Backup boot sector	Reserved												
40	Phys Drive num	0x00	Extd boot sig	Volume Serial Number			Volume Label (deprecated) normally "NO NAME "									
50	Vol Label			System ID "FAT32"					Boot code							
60	Boot code															
70																
80																
90																
…																
1D0																
1E0																
1F0															55	AA

https://www.writeblocked.org/resources/FAT_cheatsheet.pdf

Files and Directories

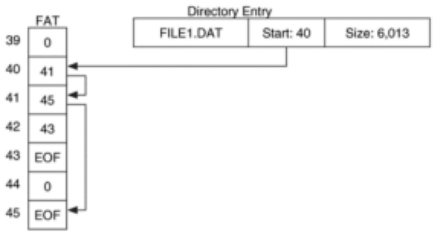
A directory entry in FAT file systems is a 32-byte record that stores metadata about a file or directory.

FAT Directory Entry

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	File name								Extension			attr ibute	reserved	10ms create time[1]	create time	
10	create date		last access date		unused		modified time		modified date		start cluster		File Size			

1. The 10millisecond create time is technically only used in FAT32.

The File Allocation Table (FAT) keeps track of file storage using cluster chains. Each file's data is stored in clusters, and the FAT table links these clusters together to form a chain.



- Each FAT entry points to the next cluster in the file's.
- Clusters marked EOF (End of File) indicate the last cluster of a file.

`fsstat` decodes this chains (in sectors); special values:

```
0 → not allocated
0xf...ff0-0xf...f6 → reserved
0xf...ff7 → damaged
0xf...ff8-0xf...fff → EOF
```

Note: FAT entries start at 0, but:

- The first addressable cluster #2.

- Entry 0 typically stores a copy of the media type, and entry 1 stores the dirty-status of the file system

Example

In eighties.dd (SHA256: cc121c3a…) and eighties-all-files.dd (SHA256:e5f16884…) you'll find two very similar FAT16 (not VFAT) file systems. In the former all files have been deleted. Using ImHex.

1. find out: Sector and cluster sizes Number of reserved sectors Locations of: FAT1, FAT2, Root Dir. (=Data Area), first cluster (#2)

compare these results with the output of fsstat

2. check the FAT entries for 48.gif in the two dd-images, and compare the results of istat on "inode" 5

```
fls -r eighties-all-files.dd
  ##OUT##
  d/d 3:  jpgs
  + r/r 517:      clive.jpg
  + r/r 518:      48k.jpg
  d/d 4:  games
  + r/r 581:      mmonty.tzx
  r/r 5:  48.gif
  r/r 6:  48.txt
  v/v 523203:     $MBR
  v/v 523204:     $FAT1
  v/v 523205:     $FAT2
  V/V 523206:     $OrphanFiles
  ###

istat eighties-all-files.dd 5
  ##OUT##
  Sectors:
  108 109 110 111 116 0 0 0 #l'ha recuperato dentro la FAT
  ###

fsstat eighties-all-files.dd

  ##OUT##
  FAT CONTENTS (in sectors)

  100-103 (4) -> EOF
  104-107 (4) -> EOF
  108-111 (4) -> 116 # cluster chain
  112-115 (4) -> EOF
  116-119 (4) -> EOF
  120-331 (212) -> EOF
  332-1211 (880) -> EOF
  1212-1279 (68) -> EOF
  ###
```

When a file name exceeds the 8.3 format, the file system creates additional directory entries to store the name in Unicode (2 bytes per character).

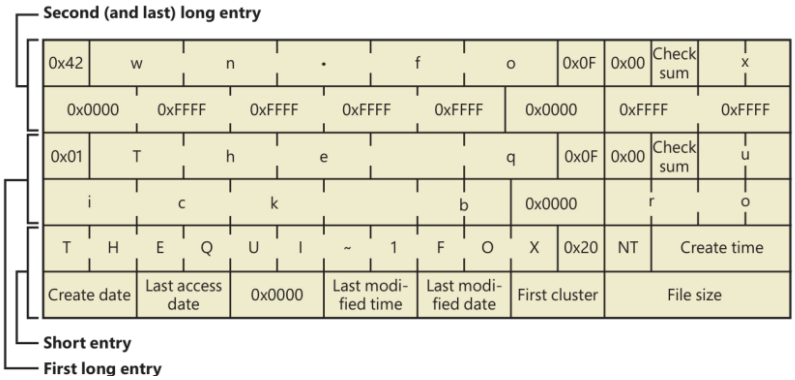
These LFN entries are linked together and precede the main directory entry (which still stores the short 8.3 name for compatibility).

- Each LFN entry is marked with the attribute 0x0F, meaning it is not treated as a normal file entry.
- The last LFN entry in the sequence has its sequence number OR-ed with 0x40; or 0xe5 if unallocated.

Long File Name

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	file name (Unicode 2 bytes/char)											0x0F	reserved	Check sum	file name	
10	file name										0x0000		file name			

The quick brown.fox", as THEQUI~1.FOX in 8.3 convention.



When a new directory is created, it contains

. and ..

Cluster 110

Name	Created	Cluster
dir2	3/30/04 01:29:01	128
dir1	4/03/04 11:47:40	196
file8.dat	3/30/04 20:41:12	112

Cluster 196

Name	Created	Cluster
.	4/1/04 09:27:00	196
..	4/1/04 09:27:00	110
file1.dat	4/3/04 12:58:23	297

those entries can be helpful for carving deleted directories

A)

Cluster 45

.	45
..	26
bad.jpg	105
dir1	210
good.jpg	153

Cluster 210

.	210
..	45
file1.txt	211
file2.txt	250
file3.txt	273

B)

Cluster 45

.	45
..	26
bad.jpg	105
newfile	**400**
good.jpg	153

Cluster 210

.	210
..	45
file1.txt	211
file2.txt	250
file3.txt	273

Since the size of a directory is always 0, the only way to know how many cluster to read is following the cluster chain

Example

In eighties-vfat.dd (SHA256: 62258f92ebb42226…) and eighties-vfat-all-files.dd (SHA256: fe46141b98d227cb…) you'll find two very similar, and familiar, VFAT FAT16 file systems. As with the previous exercise, in the former all files have been deleted.

Yet, fls -rp eighties-vfat.dd can show the full, long name, for some deleted files but not for others, that are listed under $OrphanFiles.

1. Can you explain why? Hint: eighties-vfat-all-files.dd contains some clues

In some cases, even if the file is cacelled, we have the full name, and it is strange because in the fat one byte '_' is put above the first character (eighties.dd). Since we have a vfat there are the entries with the long name and we can trace the original name. OrphanFiles is a standrd used by TSK when it does not have babstanz ainomraizons to know where that file is.

2. Using ImHex, can you manually recover the full names from eighties-vfat.dd?

```
fls -rp eighties-vfat.dd
  ##OUT##
  r/r * 3:        _
  r/r * 4:        _
  d/d * 6:        Games
  r/r * 583:      Games/Mutant Monty.tzx
  r/r * 7:        _8.gif
  r/r * 8:        _8.txt
  v/v 523203:     $MBR
  v/v 523204:     $FAT1
  v/v 523205:     $FAT2
  V/V 523206:     $OrphanFiles
  -/r * 519:      $OrphanFiles/_LIVES~1.JPG
  -/r * 520:      $OrphanFiles/_8k.jpg
  ###
```

NTFS

New Technology File System (NTFS) is a proprietary journaling file system developed by Microsoft in 1993, supporting:

- Access Control Lists (ACLs)
- Encryption
- Transparent compression
- Sparse files
- Journaling
- POSIX support (no, not WSL)
- Multiple data streams

A nice feature is that everything is a file!

- Except for the Volume Boot Record (VBR), everything else is considered a data area.
- Any sector (except VBR) can be allocated to a file.
- A very scalable design where internal structures can change over time.
- Generic data structures embed specific content.

Each unit of information associated with a file is implemented as a file attribute (NTFS Object Attribute). Each attribute consists of a byte stream.

Key points about NTFS attributes:

- The contents of a file are treated as 'an attribute,' similar to its name or timestamps.
- Each file has a special `$DATA` attribute with no name that corresponds to its content.

Applications can create additional named streams, called Alternate Data Streams (ADS).

- For example, the `$Zone.Identifier` is used by Windows to mark files downloaded from the web.

- You can list ADSs using `dir /r` or tools like `streams`.
- You can set or show their contents by redirecting commands like `echo` and `more`.

When mounting NTFS file systems, consider specifying:

- `show_sys_files` to display metafiles in directory listings.
- `streams_interface=windows` to access ADS like in Windows.

Refer to `mount.ntfs(8)` for more details.

Hard links allow multiple paths to refer to the same file (not directory):

```
mklink /h new-name existing-name
```

- Similar to Unix, they are reference-counted and limited to the same file system.

Soft links are strings interpreted dynamically and can point to files, directories, or non-existent targets:

```
mklink new-name existing-name
```

- Implemented as reparse points (files or directories containing application-specific reparse data and a 32-bit reparse tag).

Junctions are a legacy concept, functioning almost identically to directory symbolic links. See [ARIS21] for more details.

Shortcuts are `.lnk` files interpreted by Explorer.

Volume Organization

NTFS maps the entire volume into clusters, which are the smallest allocatable units of storage.

This is different from FAT, which uses a simpler allocation table.

The cluster factor (size of a cluster) depends on the size of the volume.
It is an integral number of physical sectors and always a power of 2.

- Larger clusters:
  - Reduce fragmentation.
  - Speed up allocation.
  - However, they can lead to *wasted space* (internal fragmentation) when storing small files.

1. Logical Cluster Numbers (LCNs)

LCNs are used to number clusters sequentially from the beginning of the volume.
They represent the physical location of clusters on the disk.

2. Virtual Cluster Numbers (VCNs)

VCNs are used to address data within a file.
They represent the logical view of a file's data.
VCNs are not necessarily physically contiguous, allowing NTFS to handle fragmented files efficiently.

Volume Layout

0–2	Assembly instruction to jump to boot code	No (unless it is the bootable file system)
3–10	OEM Name	No
11–12	Bytes per sector	Yes
13–13	Sectors per cluster	Yes
14–15	Reserved sectors (Microsoft says it must be 0)	No
16–20	Unused (Microsoft says it must be 0)	No
21–21	Media descriptor	No
22–23	Unused (Microsoft says it must be 0)	No
24–31	Unused (Microsoft says it is not checked)	No
32–35	Unused (Microsoft says it must be 0)	No
36–39	Unused (Microsoft says it is not checked)	No
40–47	Total sectors in file system	Yes
48–55	Starting cluster address of MFT	Yes
56–63	Starting cluster address of MFT Mirror $DATA attribute	No
64–64	Size of file record (MFT entry)	Yes
65–67	Unused	No
68–68	Size of index record	Yes
69–71	Unused	No
72–79	Serial number	No
80–83	Unused	No
84–509	Boot code	No

8-

1. No Fixed Layout:
   - NTFS does not have a fixed layout for the volume, except for the Volume Boot Record (VBR).
   - The VBR contains information that guides the system to the MFT, which is the core of NTFS.
2. 8-bit Sizes Interpretation:
   - Sizes in NTFS are represented as 8-bit values.
   - Positive values indicate the number of clusters.
   - Negative values are interpreted as 2^n, where `n` is the negative value.

Master File Table The MFT is the heart of the NTFS volume structure. It is implemented as an array of file records (similar to inodes). Key details include:

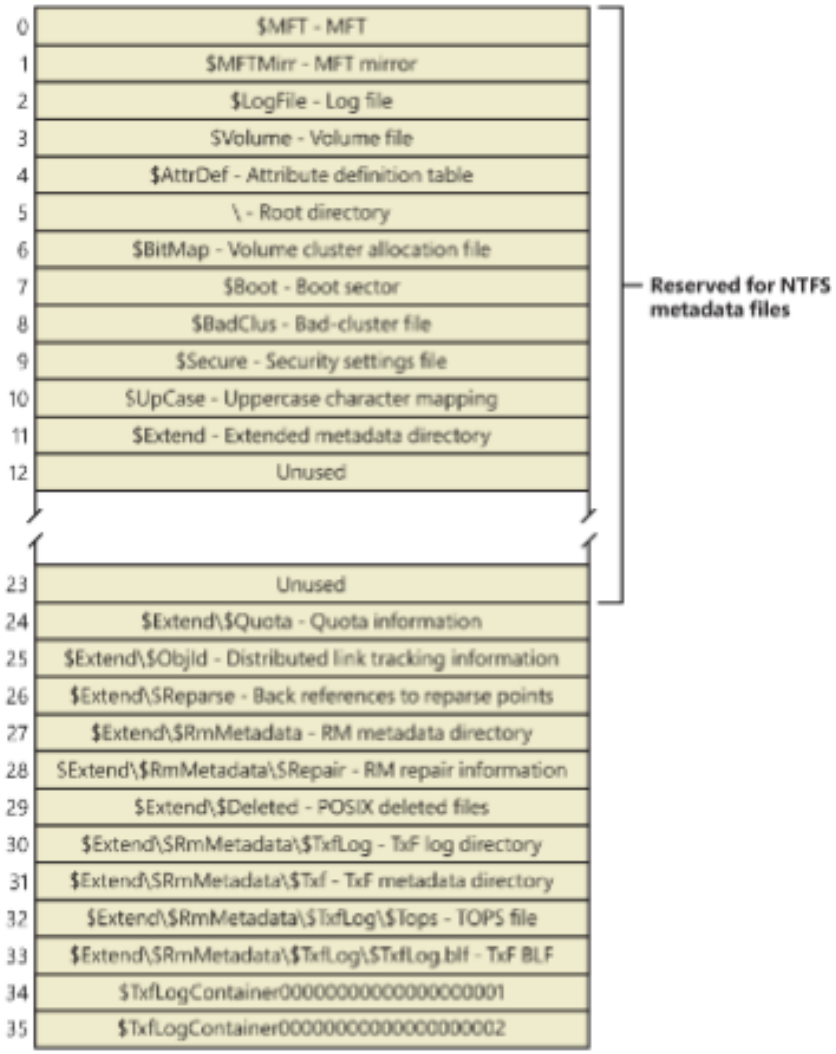
- The size of each record can be defined at format time (typically 1 KB or 4 KB).
- The size depends on the underlying physical medium:
  - Disks with 4 KB sector sizes generally use 4 KB file records.
  - Older disks with 512-byte sectors use 1 KB file records.
- The size does not depend on the cluster size.

When a file needs more metadata space, the base file record stores the location of additional records. The MFT's location is specified in the BIOS Parameter Block inside the VBR.

Key points about the MFT:

- The MFT contains one record for each file, including itself (the first entry).
- It can be fragmented; however, an MFT zone is typically reserved during formatting (about 12.5% of the entire volume).
- In addition to file records, there are other system metadata files. These hidden files have names that begin with a dollar sign ($).

File records for metadata files These metadata are 'special files' recorded in the first MFT records.



NTFS incorporates fixup values into data structures that are over one sector in length.

This is used to check the integrity of sectors during reading. This protects against hardware errors (e.g. corrupted sectors).

- the last two bytes of each sector(512byte) are replaced with a "signature" value
- the signature is later used to verify the integrity of the data

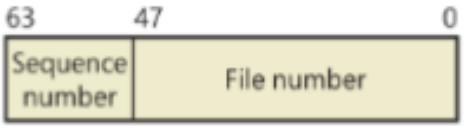
Fixups are only in data structures, not in sectors with file content

The "signature" is incremented each time the structure is updated

File identifiers

Files identified by 64-bit "file record numbers", which consist of:

1. a file number, corresponding to the (0-based) position in the MFT
2. a sequence number, incremented when a file record is reused (i.e. if the file is deleted and the record reused for a new file)



MFT Entries

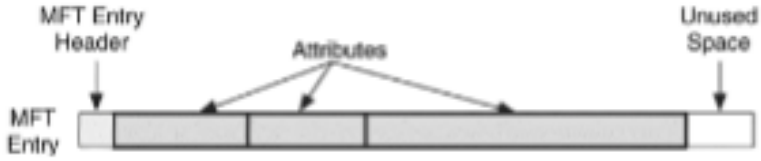
File records start with a fixed header:

File Record Segment Header

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	F	I	L	E	Update Seq array offset		Update Seq array size		$LogFile Sequence Number							
1	Seq no		Hard Link Count		1 attrib offset		Flags		Used size of file record				Allocated size of file record			
2	File reference to base file record								Next attrib ID				MFT Record No			

followed by attributes (and fixup values):

('Update Seq == fix-up) NTFS Cheat Sheets



Residient Attribtues

In NTFS, each file or folder is a record in the Master File Table (MFT). Each record consists of a series of attributes, which describe the characteristics of the file.

- `$STANDARD_INFORMATION`: Timestamps, flags, UID, etc.
- `$FILE_NAME`: File name and parent directory.
- `$DATA`: File content.
- `$SECURITY_DESCRIPTOR`: Permissions. ...

Attributes are "resident" if their value is stored directly in the MFT record.

EXT

The Ext (Extended) file system family—Ext2, Ext3, and Ext4—is a series of filesystems used in Linux. These are based on the traditional Unix File System (UFS), but add several modern capabilities over time.

Key Modern Features:

- Extended Attributes / POSIX ACLs: Allow more detailed permissions than traditional Unix read/write/execute.
- Journaling (from Ext3 onwards): Keeps a log (journal) of changes to help recover quickly after crashes.
- Encryption: Protects file contents and filenames (introduced in Ext4).
- 64-bit Support: Allows management of much larger files and filesystems.
- More...

The Ext file systems are modular, with features grouped by their compatibility level:

Feature Type	What It Means	Example
Compatible	If not supported, OS can still mount the FS normally	has_journal
Incompatible	If not supported, OS must not mount the FS	encrypt
Read-Only Compatible	If not supported, OS can mount in read-only mode	dir_index

Support for Very Large Volumes

- Ext3: Limited to volumes up to 16 TB (terabytes), calculated as $16 \cdot 10^{12}/2^{44}$.
- Ext4: Extends this limit to 1 exabyte (EB), or $10^{18}/2^{60}$. This makes Ext4 suitable for modern systems with very high storage demands.

Maximum File Size

- Ext3: The maximum size of a single file is 2 TB.
- Ext4: Increases this limit to 16 TB, making it more suitable for applications requiring the management of large files.

Backward Compatibility

- Ext4: Can mount Ext3 file systems and treat them as Ext4. This process is called "on-the-fly conversion": existing files remain in the Ext3 format, but new files will use Ext4's advanced features.
- Ext3: Cannot mount Ext4 file systems, as Ext3 does not support the new features introduced in Ext4.

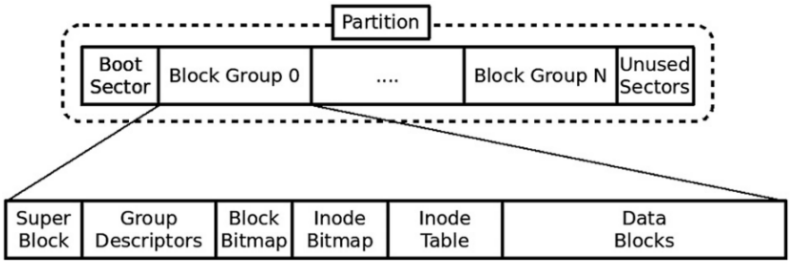
Extents

Ext4 uses a structure called extents to map data blocks more efficiently. Extents represent a continuous range of blocks, reducing fragmentation and improving performance. This approach is similar to the one used by NTFS (the Windows file system).

Layout

In the Ext file system family (Ext2, Ext3, Ext4):

- Sectors (the smallest physical units on a disk, typically 512 bytes) are grouped into blocks of 1, 2, or 4 KB.
- These blocks are conceptually similar to "clusters" in FAT or NTFS.
- Unlike the Unix File System (UFS), Ext does not assemble blocks from smaller "fragments." in Ext, the terms "block" and "fragment" are essentially synonymous (the term "block" is predominantly used).
- The superblock is located at an offset of 1024 bytes from the start of the volume (not at the very beginning). It contains all the fundamental parameters of the file system.
- The size of the superblock is 1024 bytes. An optional reserved area may follow the superblock.
- Boot code, if present, resides in the Master Boot Record (MBR) or Volume Boot Record (VBR), not within the file system itself.
- The rest of the file system is divided into block groups.



A key detail: when the first block group (BG0) starts at offset 0:

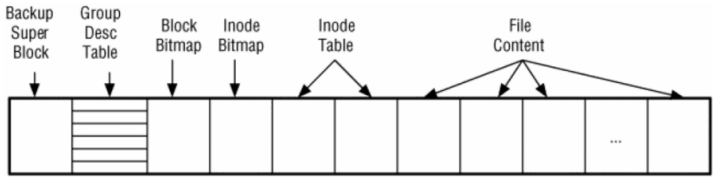
- The primary superblock is located at an offset of 1024 bytes from the volume start (or within block 0).
- Backup copies of the superblock (if present) are located at the beginning of other block groups (BG1, BG2, etc.).

Each "copy" of the superblock has its own specific metadata.

- This backup structure, with superblock copies in multiple locations, is a critical safety feature that allows recovery even if parts of the file system are damaged.

Each block group

1. contains its data bitmap, inode bitmap, inode table, data blocks
2. may contain the backup of the superblock and the GD table



Each group descriptor defines where to find the components of the block group.

- The main group descriptor table is located in the block immediately following the superblock.
- This table can be copied, after the superblock backup, to all or some groups, depending on the formatting options (see `sparse_super[2]` in the `ext4(5)` man page).

Ext4 introduces advanced options for managing metadata and resizing:

- flexible block groups (`flex_bg`): allows block group metadata to be placed anywhere, not necessarily within the same group.
- reserved GDT blocks: enables online resizing of the file system without requiring it to be unmounted.

Standard command `dumpe2fs` prints superblock and group information.

- All groups, except for the last, contain the same number of blocks n
- by default, n is equal to the # of bits in a block: per blocchi di 4 KB (4096 byte), ogni blocco contiene 32.768 bit (4096 × 8), quindi ogni gruppo può gestire 32.768 blocchi
  - the block bitmap is exactly 1 block
- the # of inodes can be chosen at format time, usually less than n

---

Example

Use `dumpe2fs/fsstat` to list

- block size = 2048 byte
- blocks and inodes per group = 888;296
- number of groups = 18

in the image linus-ext2.dd (SHA256: b6b1836ff1efef3a70…)

- Are there unused sector after the FS? no total size of fs == 16384*2048 == stat -c %s linus-ext2.dd
- All are group of the same size? no, the end group have a size of 400 blocks

---

Unused space

- The first 1024 bytes are not technically used
- There are unused bytes in the superblock
- There can be unused entries in the GD-table
  - Or they backup copies
- There are the reserved GDT blocks

Those are possible places where to hide data

Superblock details

Byte Range	Description	Essential
0–3	Number of inodes in file system	**Yes**
4–7	Number of blocks in file system	**Yes**
8–11	Number of blocks reserved to prevent file system from filling up	No
12–15	Number of unallocated blocks	No
16–19	Number of unallocated inodes	No
20–23	Block where block group 0 starts	**Yes**
24–27	Block size (saved as the number of places to shift 1,024 to the left)	**Yes**
28–31	Fragment size (saved as the number of bits to shift 1,024 to the left)	**Yes**
32–35	Number of blocks in each block group	**Yes**
36–39	Number of fragments in each block group	**Yes**
40–43	Number of inodes in each block group	**Yes**
44–47	Last mount time	No
48–51	Last written time	No
52–53	Current mount count	No
54–55	Maximum mount count	No
56–57	Signature (0xef53)	No
58–59	File system state (see Table 15.2)	No
60–61	Error handling method (see Table 15.3)	No
62–63	Minor version	No
64–67	Last consistency check time	No
68–71	Interval between forced consistency checks	No
72–75	Creator OS (see Table 15.4)	No
76–79	Major version (see Table 15.5)	**Yes**
80–81	UID that can use reserved blocks	No
82–83	GID that can use reserved blocks	No
84–87	First non-reserved inode in file system	No
88–89	Size of each inode structure	**Yes**
90–91	Block group that this superblock is part of (if backup copy)	No
92–95	Compatible feature flags (see Table 15.6)	No
96–99	Incompatible feature flags (see Table 15.7)	**Yes**
100–103	Read only feature flags (see Table 15.8)	No
104–119	File system ID	No
120–135	Volume name	No
136–199	Path where last mounted on	No
200–203	Algorithm usage bitmap	No
204–204	Number of blocks to preallocate for files	No
205–205	Number of blocks to preallocate for directories	No
206–207	Unused	No
208–223	Journal ID	No
224–227	Journal inode	No
228–231	Journal device	No

Byte Range	Description	Essential
232–235	Head of orphan inode list	No
236–1023	Unused	No

Example

1. use `dumpe2fs/fsstat` to check where the superblock copies are
2. dump the first three, and compare them: are they equal?
    - note: the main SB starts at offset 1024, the others at 0
    - are the 2nd and 3rd equal?

```
dumpe2fs linus-ext2.dd | grep "superblock"
    ##OUT##
    Primary superblock at 0, Group descriptors at 1-1
    Backup superblock at 888, Group descriptors at 889-889
    Backup superblock at 2664, Group descriptors at 2665-2665
    Backup superblock at 4440, Group descriptors at 4441-4441
    Backup superblock at 6216, Group descriptors at 6217-6217
    Backup superblock at 7992, Group descriptors at 7993-7993
    ###
#The primary superblock is located after the boot block
# the superblock, at volume offset 1024, contains the FS parameters
# the superblock is 1024 bytes in size
dd if=linus-ext2.dd bs=1k skip=1 count=1 of=sb1

#To convert from filesystem block (2048) numbers to 1KB blocks for dd, you need to multiply by 2:
dd if=linus-ext2.dd bs=1k skip=$((888*2)) count=1 of=sb2
dd if=linus-ext2.dd bs=1k skip=$((2664*2)) count=1 of=sb3

md5sum sb1 sb2 sb3
    ##OUT##
    922c7935bd45a7b36fc938f3b000d16c  sb1
    06469d508b7da81f55e090addf908598  sb2
    5858141cac833da5d7a0195dfd968119  sb3
    ###


vbindiff sb2 sb3

    ###
    change the bit that keeps track of the superblock group membership
    ###

vbindiff sb1 sb3
    ###
    more diversity because the primary superblock
    also tines the last path where the fs was mounted (not essential)
    ###
```

Group descriptors details

Byte Range	Description	Essential
0–3	Starting block address of block bitmap	**Yes**
4–7	Starting block address of inode bitmap	**Yes**
8–11	Starting block address of inode table	**Yes**
12–13	Number of unallocated blocks in group	No
14–15	Number of unallocated inodes in group	No
16–17	Number of directories in group	No
18–31	Unused	No

Inode

Inodes are the primary metadata structure.

- fixed size, defined in the superblock, minimum 128 bytes (`dumpe2fs -h linus-ext2.dd | grep "Inode size"`)
- extra-space can be used to store extended attributes (otherwise, data blocks are used)
- small non-user content can be stored inside direct-block pointer array; e.g., symlink values
- each inode has a unique 'address' or number, starting with 1 (index 0 is not used)
- The inodes of each block group are stored in a table and the position of this table is specified in the block descriptor
- The allocation status of each inode is determined via the inode bitmap nd the position of this table is specified in the block descriptor

Standard commands can be used to inspect the FS:ù

- `-i`,`-lai` in `ls`, shows inode-numbers
- `stat` shows some metadata

debugfs is a FS "debugger" that can display a lot of information.

```
ln pippo.txt pippo-hardlink.txt
ln -s pippo.txt pippo-hardlink.txt
ls -li
    ##OUT##
    1445743 -rw-r--r--  2 root    root       0 Apr  3 10:20 pippo-hardlink.txt
    1445746 lrwxrwxrwx  1 root    root       9 Apr  3 10:42 pippo-symblink.txt -> pippo.txt
    1445743 -rw-r--r--  2 root    root       0 Apr  3 10:20 pippo.txt
    ###

    ###
    for symb link we get differen inode number beacsue is
    the newfile and fs must allocated a new inode and
    content for symb link. The contet of ippo-symblink.txt is the path " -> pippo.txt",
    that just a string that is resolved we we tryb to open the pippo-symblink.txt.
    ###
```

Inodes 1 to 10 are reserved

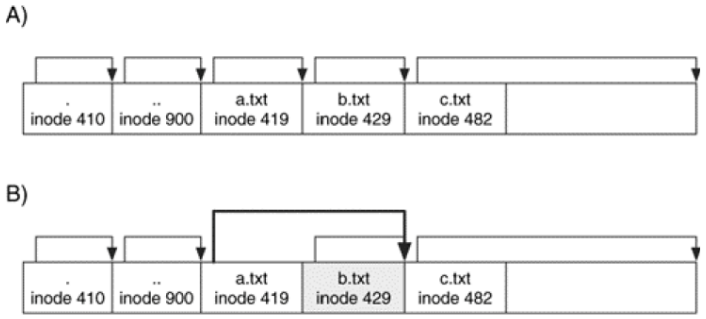
- 1 is (was?) used for keeping track of bad blocks
- 2 is used for the root directory
- 8 is typically for the journal

Byte Range	Description	Essential
0–1	File mode (type and permissions)	**Yes**
2–3	Lower 16 bits of user ID	No
4–7	Lower 32 bits of size in bytes	**Yes**
8–11	Access Time	No
12–15	Change Time	No
16–19	Modification time	No
20–23	Deletion time	No
24–25	Lower 16 bits of group ID	No
26–27	Link count	No
28–31	Sector count	No
32–35	Flags	No
36–39	Unused	No
40–87	12 direct block pointers	**Yes**
88–91	1 single indirect block pointer	**Yes**
92–95	1 double indirect block pointer	**Yes**
96–99	1 triple indirect block pointer	**Yes**
100–103	Generation number (NFS)	No
104–107	Extended attribute block (File ACL)	No
108–111	Upper 32 bits of size / Directory ACL	No
112–115	Block address of fragment	No
116–116	Fragment index in block	No
117–117	Fragment size	No
118–119	Unused	No
120–121	Upper 16 bits of user ID	No
122–123	Upper 16 bits of group ID	No
124–127	Unused	No

Directories

The old directory entry was a simple data structure containing

- the file name (variable length, 1-255 chars) where the length of an entry is rounded up to a multiple of four
- the inode number (AKA index+1)



The newer one uses one byte in the filename-length to store the file type.

Allows detecting when an inode has been reassigned (reallocated)!

Byte Range	Description	Essential
0–3	Inode value	**Yes**
4–5	Length of this entry	**Yes**
6–6	Name length	**Yes**
7–7	File type	No
8+	Name in ASCII	**Yes**

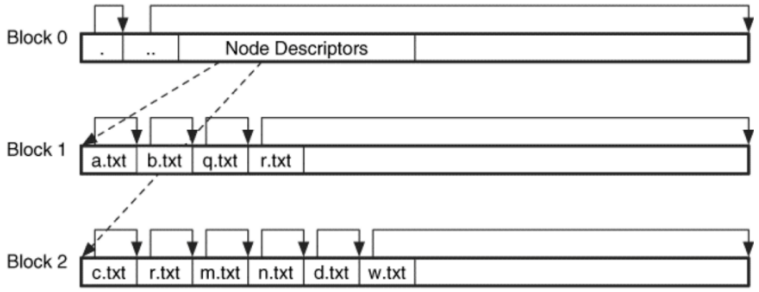
File Type	Description
1	Regular file
2	Directory
3	Character device
4	Block device
5	FIFO
6	Unix Socket
7	Symbolic link

In ext3 and ext4, option `dir_index` allows the FS to use hashed B-trees to speed up name lookups

- similar to NTFS: This approach is conceptually similar to that used by NTFS in Windows
- when this functionality is active, a `ro-compatible` (read-only compatible) flag is set in the superblock (This means that systems that do not support this function can still mount the file system, but only in read-only mode)

Still the same directory-entry structures, but in sorted order

- each entry continues to have the same format and contain the same information (Inode value, Length of this entry ...) but instead of storing the entries in a linear manner (one after the other), the entries are organised in a B-tree structure



Example

List files in the root directory of linus-ext2.dd by

- (ro) mounting it
- using TSK's fls
- using ImHex
  - get the block-size from the SB == 1 (=1K)
  - the GD-table is in the block after the SB
  - decode the first GD and get the block for the (first) inode-table
  - the inode n.2 (index 1) is for the root directory
  - the first direct-block-pointer points to the beginning of the directory

- decode the directory entries

```
mount -oro  linus-ext2.dd mnt/linus-ext2
ls -li
    ##OUT##
    total 28
    12 -rw-r----- 2 root root   773 Apr  8  2023 hard_link.txt
    12 -rw-r----- 2 root root   773 Apr  8  2023 linus.txt
    15 lrwxrwxrwx 1 root root   109 Apr  9  2023 long_symlink -> /media/someuser/whatever/subdir1/subdi
    11 drwx------ 2 root root 16384 Apr  8  2023 lost+found
    5033 drwxr-xr-x 4 root root  2048 Apr  8  2023 pics
    13 lrwxrwxrwx 1 root root     4 Apr  8  2023 pictures -> pics
    14 -rw-r--r-- 1 root root     8 Apr  9  2023 very_short_text.txt
    ###

fls -rp linus-ext2.dd
    ##OUT##
    d/d 11: lost+found
    d/d 5033:       pics
    d/d 5034:       pics/tux
    r/r 5040:       pics/tux/tux-lego.png
    r/r 5041:       pics/tux/tux-windows.png
    r/r 5042:       pics/tux/tux.png
    d/d 5035:       pics/linus
    r/r 5036:       pics/linus/linus_2018.jpg
    r/r 12: linus.txt
    l/l 13: pictures
    r/r 12: hard_link.txt
    r/r 14: very_short_text.txt
    l/l 15: long_symlink
    V/V 5625:       $OrphanFiles
    -/r * 5037:     $OrphanFiles/OrphanFile-5037
    -/r * 5038:     $OrphanFiles/OrphanFile-5038
    -/r * 5039:     $OrphanFiles/OrphanFile-5039
    ###
```

Extended

Extended attributes are an advanced feature of Ext file systems (Ext2/3/4) that allows additional metadata to be associated with files and directories. This metadata is stored as name-value pairs.

- Ogni attributo è una coppia composta da:
  - Name: specified in the `namespace.attribute-name format` (current namespaces are security, system, trusted, and user)
  - Value: An arbitrary datum associated with the name

Gli attributi estesi sono utilizzati per implementare le Access Control Lists (ACL), che consentono di definire permessi più dettagliati rispetto ai tradizionali permessi Unix.

```
setfacl -m u:username:rwx file.txt  # Set up an ACL
getfacl file.txt                    # View ACLs
```

kernel and filesystem may place limits on the maximum number and size of extended attributes that can be associated with a file

Extended attributes are stored in a separate block associated with the file. If several files share the same attributes, they can use the same block to optimise space.

```
getfattr -d file.txt # Display extended attributes

# set an extended attribute
setfattr -n user.comment -v "This is an important file" file.txt
setfattr -x user.comment file.txt # setfattr -x user.comment file.txt
```

See xattr(7)

Network Forensics

Network forensics is a sub-branch of digital forensics relating to the monitoring and analysis of computer network traffic for the purposes of information gathering, legal evidence, or intrusion detection.

- Shift to network-centric computing

  Computing has evolved from isolated computers to network-centered systems as people rely on networks for various activities

- Importance of following the cybertrail

  Digital investigators must now trace evidence across networks including the public Internet, private networks, and commercial systems to collect relevant digital evidence

Process

The investigation process identifies communicating hosts in terms of time, frequency, protocol, application, and data. It tries to answer the 5W and 1H

- **Who**: identifying the source

  determining who is behind an attack or suspicious activity by identifying originating hosts or users

- **What**: identifying the payload and activities

  identifying exactly what data or malicious payloads are being transmitted

- **Where**: determining the destination or target

  identifying which users, systems, or resources are being targeted or have been compromised

- **When**: establishing a timeline

  defining the exact timeframe of events to reconstruct incident progression

- **Why**: understanding motivation and intent

  determining the attacker's goal (gaining initial access, obtaining credentials or escalating privileges, collecting specific sensitive data, establishing persistence, lateral movement, . . .)

- **How**: techniques and methods used

  understanding the attacker's methodology, tactics, and specific exploits

he 5Ws and 1H framework is always relevant and necessary at every investigative step (or for homogeneous groups of steps)

Applying this framework systematically ensures completeness, consistency, and analytical rigor, enabling investigators to precisely reconstruct the timeline of an attack

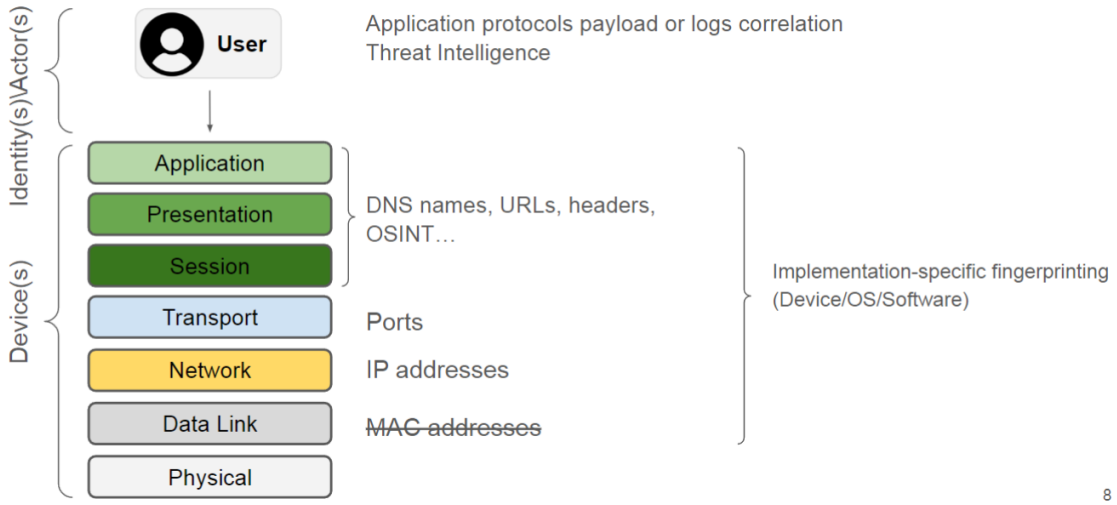
When	Who	What	Where	Why	How
2024-03-28 03:15 AM	IP: 1.2.3.4 User: Unknown	Initial unauthorized access attempt (login)	IP: 10.0.2.20 (Webserver, port 443)	Gaining initial foothold in network	Exploiting known vulnerability (RCE on web application)
2024-03-28 03:20 AM	IP: 10.0.2.20 (compromised Webserver)	Lateral movement attempt via SSH	IP: 10.0.3.15 (Internal DB Server, port 22)	Access to sensitive database data	Exploitation of SSH credentials (private key on 10.0.2.20)
...	...	...	...	...	...

Report (a possible structure)

There is no single "official" format for network forensics reports

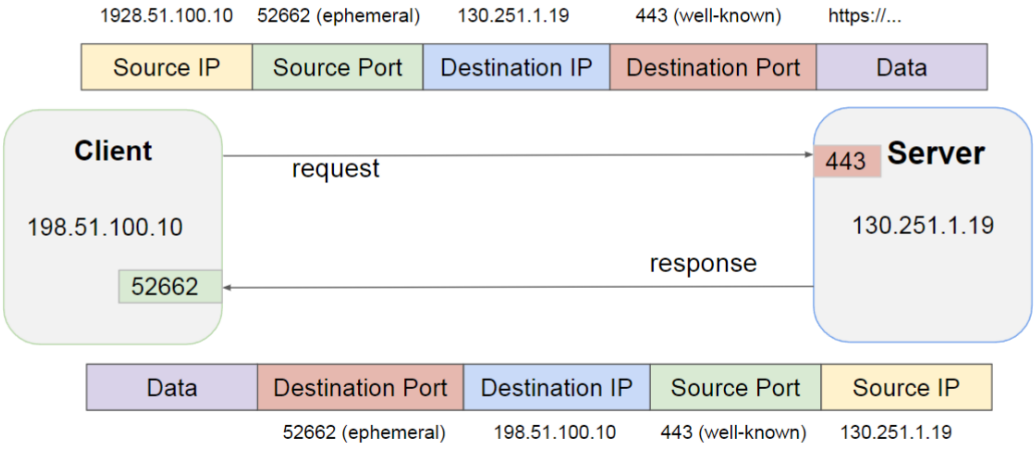
- An overview of the investigation objectives
- A recap of events
- What digital forensics tools (and methodologies) have been used
- Detailed timeline
- Clearly identify each artifact and include its cryptographic hash
- Recommendations and mitigations
- Suggest improvements to security processes based on lessons learned from the incident

Who(/Where)



MAC addresses (crossed out) – once useful for identifying local devices, but:

- They're not preserved across networks (only visible on the same LAN)
- Easily spoofed or obfuscated (e.g., by VPNs or virtual interfaces)



ayer 4 is in charge of the process-to-process communication. Transmitter and receiver are identified using ports

16-bit unsigned integer (0-65535, 0 reserved) conventionally divided into:

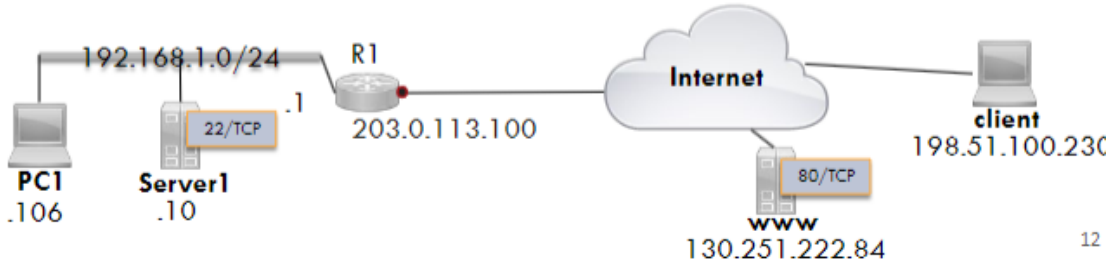
- Well-known ports (0-1023): used by system processes that provide widely used types of network services (requires superuser privileges)
- Registered ports(1024-49151): assigned by a central authority (the Internet Assigned Numbers Authority, IANA) for specific services
- Ephemeral ports(49152–65535): contains dynamic or private ports that cannot be registered with IANA

(see /etc/services)

Source NAT and Masquerade

Network Address Translation (NAT) generally involves rewriting the source and/or destination addresses of IP packets as they pass through a router or firewall

- NAT affects answering Who/Where questions
  - 192.168.1.0/24 is a private network and it is not routable on the Internet
- Masquerade is a source NAT rule, i.e., it is related to the source address of a packet
- The popular usage of NAT Masquerade is to translate a private address range to a single public IP address



Example:

NAT Table (Dynamic)

Public IP	Public Port, Destination Port	Private IP
203.0.113.100	52000, 80	192.168.1.106
203.0.113.100	53000, 80	192.168.1.10

1. PC1 and Server1 accessing www (request)

SRCIP	SRCPORT	DSTIP	DSTPORT		SRCIP	SRCPORT	DSTIP	DSTPORT
192.168.1.106	52000	130.251.222.84	80	R1 →	203.0.113.100	52000	130.251.222.84	80
192.168.1.10	53000	130.251.222.84	80	R1 →	203.0.113.100	53000	130.251.222.84	80

2. PC1 and Server1 accessing www (response)

SRCIP	SRCPORT	DSTIP	DSTPORT		SRCIP	SRCPORT	DSTIP	DSTPORT
130.251.222.84	80	192.168.1.106	52000	R1 ←	130.251.222.84	80	203.0.113.100	52000
130.251.222.84	80	192.168.1.10	53000	R1 ←	130.251.222.84	80	203.0.113.100	53000

Port forwarding

Port forwarding is a destination NAT rule, i.e., it is related to the destination address of a packet

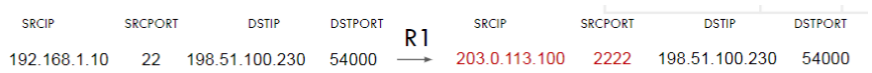
Maps external IP addresses and ports to Internal IP addresses and ports allowing access to internal services from the Internet

DNAT table (static)

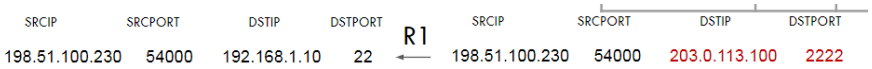
Public IP Address	Ext. Port	Private IP Address	Int. Port
203.0.113.100	2222	192.168.1.10	22

Example:

1. Client connecting to Server1 (request)



2. lient connecting to Server1 (response)



To identify internal hosts behind NAT.

1. at device translation logs (NAT table)
2. correlate ephemeral ports between pre-NAT and post-NAT sessions to identify the original internal host
3. Some protocols include internal IP information in their payloads or headers, which can help identify the internal host:
    - FTP (File Transfer Protocol) → PORT command includes the client's IP and port for data connection
    - SIP (Session Initiation Protocol) → Via: and Contact: headers may contain the internal IP address of the user agent
    - ICMP (Error messages) → Error payload includes the original IP header
    - HTTP / Custom APIs → Sometimes apps send their local IP in headers or structured payloads (e.g., JSON payload "client_ip": "192.168.1.10")

Full content data refers to every single piece of information that is transmitted over a network or networks, without any filtering or modification.

- is captured and stored in its entirety, including all the traffic that passes through the network, often referred to as packet captures or PCAP
- includes not only the payload or data portion of the network packets, but also the header information, metadata, timestamps, and any other data associated with the network communication

Session data onsists of aggregated traffic metadata and usually refers to the conversation between two network entities

- grouped together into flows and/or groups of network packets related to one another
- are able to inform the investigator about questions such as who talked to whom (who/where), when, for how long, etc. without looking at any contents of the conversation(s) at all.

```
Date first seen          Duration Proto     Src IP Addr:Port          Dst IP Addr:Port     Flags Tos  Packets    Bytes      pps      bps    Bpp Flows
2020-04-22 12:19:58.824     0.004 TCP      44.30.248.239:443   ->     44.244.6.114:54044 ...AP...  16      141   204984    35250  410.0 M   1453     1
2020-04-22 12:22:37.845     0.004 TCP       175.68.86.47:80    ->     44.244.6.114:53717 ...AP... 128      133   184649    33250  369.3 M   1388     1
2020-04-22 12:20:37.844     0.004 TCP       175.68.86.47:80    ->     44.244.6.114:53717 ...AP... 128      133   184649    33250  369.3 M   1388     1
2020-04-22 12:24:37.845     0.004 TCP       175.68.86.47:80    ->     44.244.6.114:53717 ...AP... 128      132   184609    33000  369.2 M   1398     1
```

(see https://en.wikipedia.org/wiki/NetFlow)

Specific systems, typically Network Intrusion Detections System (NIDS), trigger alerts based on

- signature-based detection: looking for specific patterns, such as byte sequences
- anomaly-based detection: studies the normal behaviour of the monitored system and then looks out for any difference in it

Mainstream open source solutions are

- SNORT https://www.snort.org/
- Suricata https://suricata.io/

Statistical data provide the analyst with network-related aspects such as

- the number of bytes contained in a packet trace
- start and end times of network conversations
- number of services and protocols being used
- most active network nodes
- least active network nodes
- outliers in network usage
- average packet size, average packet rate
- … It can therefore also act as a useful source for anomaly detection.

Correlation of different sources

Network-based evidence can be correlated with other sources to enhance forensic investigations and root cause analysis. Examples include:

1. Network Nodes:
   - Logs and files from network nodes such as attack computers, intermediate systems, or victim computers can provide critical evidence.
2. Examples of Logs:
   - *SSH Server Logs*:
     ```
     journalctl -u sshd
     Apr 15 13:45:29 server1 sshd[3859975]: Accepted publickey for user from 10.187.10.221 port 601
     ```
   - *Proxy Server Logs*:
     ```
     tail -f /var/log/squid.log
     1681571063.731 171297 93.51.10.270 TCP_TUNNEL/200 6889 CONNECT www.google.com:443 enricorusso
     ```
   - *Mail Server Logs*:
     ```
     tail -f /var/log/mail.log
     Jul 4 19:47:58 mammon postfix/smtpd[4936]: 07A1753F: client=c-69-181-123-456.hsd1.ca.comcast.n
     ```
3. Internetworking devices (e.g., router, access point, or VPN concentrators): logs and buffers

Who: IP and Domain OSINT

Investigate suspicious IP addresses and domains using publicly available sources.

- Check if an IP or domain has been reported for malicious activity
- Identify infrastructure related to known threat actors
- Gather context (geolocation, ISP, reverse DNS, historical records)

Tools:

- *VirusTotal*
  - Multi-engine scanner for IPs, domains, files
  - Shows passive DNS, related indicators, threat labels
- *AbuseIPDB*
  - Community-powered IP reputation
  - View abuse reports, threat categories, and risk scores
- *Shodan*
  - Search engine for internet-exposed devices
  - Discover open ports, banners, services running on an IP

What/How: TTPs

Tactics, Techniques, and Procedures (TTPs) describe the behavioral patterns of threat actors.

The MITRE ATT&CK framework provides a structured knowledge base of real-world.

TTPs observed across threat campaigns.

- Tactic (What): the attacker's goal or objective at a certain stage (e.g., Credential Access, Lateral Movement)
- Technique/Procedure (How): the method or implementation used to achieve that goal (e.g., Brute Force - T1110, Exploitation of Remote Services - T1210)

How: CWE and CVE

- *Common Weakness Enumeration (CWE)*:
  - Represents a general weakness (e.g., improper input validation).
  - A community-developed knowledge base of common software and hardware weaknesses, maintained by MITRE.
  - If you only identify a CWE, you still understand what kind of mistake allowed the attack.
- *Common Vulnerabilities and Exposures (CVE)*:
  - Identifies a specific vulnerability in a real product (e.g., a buffer overflow in OpenSSL version X.Y).
  - If you know the CVE, you know exactly which hole the attacker used.
  - Searching for CVEs
    * NVD (National Vulnerability Database)
    * MITRE CVE site
    * Exploit DB
    * [Google/GitHub search + product/version or artifacts]

Collecting network-based evidence

The task of acquiring network evidence can be divided into active and passive acquisition.

- passive acquisition: refers to gathering data without emitting data at OSI Layer 2 or above, such as capturing or sniffing network traffic.
- active acquisition: involves interacting with systems on the network, such as sending queries or logging to a central host, SIEM, or management station, and may also include scanning network ports to determine system status

To preserve as much of the evidence as possible, acquisition should not change the packets, send out additional packets or alter the network configuration.

Passive acquisition

Network forensic investigators can passively acquire network traffic by

- intercepting it as it is sent across cables
- through network equipment such as (hubs) and switches
- through the air