# Notas Forense

## Slide 1 Overview:

CIA -> confidentiality, integrity and availability
AAA -> authentication, authorization e accounting

Cybercrime vs Computer crime -> Computer crime violates CIA or AAA, and cybercrime is any crime that is committed in the cyberspace

Ler aquelas leis todas

Digital evidence:
- Must be obtained in a legal way
- Technically irrefutable

## Slide 2 Digital Forensics:

Focus of Digital investigation:
- digital devices involved in a crime
- devices that commited a crime or a digital event that violates a policy or law

Digital investigation is a scientific method used to test and validate or refute a hypothesis.

Digital evidence is an object that contains reliable information.
Must be admissible, authentic, accurate and complete.

Forensic means it can be used in court of law, and the investigation is more restricted because of it.

Type of analysis:
- live - while it is running
- post-mortem - on a controlled environment

Digital Crime Scene Investigation Methodology:

1- Identify the digital evidence and choose the best approach to analyze it.
2- Preserve evidence and reduce the lost information, using write blockers and backups or full copies of information. Use hashes to preserve the data integrity, or digital signatures.
3- Evidence searching finds data that supports or refutes an hypothesis. Search for file extensions, common locations, metadata, packets etc.
4- Event reconstruction and report, correlate digital events with physical events and reconstruct events that happened and how, after reporting all findings.

Digital Evidence handling:

1- Identify data state and data sources (main data types)
2- Preserve evidence and reduce the lost information, using backups or full copies of information. Use hashes to preserve the data integrity, or digital signatures. Sort the data that is useful.
3- Isolate by using vms to run potencial malicious software or html files.
4- Correlate data with other independent sources, as data can be forged.
5- Log all actions of the analysis, identify devices, information and tagging rules.

Ethical code - nao esconder provas, nao mentir, nao revelar info confidencial, nao fazer nada de ilegal, etico e moral etc.

## Slide 3 Obtaining Evidence:

Use a forensic boot device on the computer, so that the storage drive is not altered during the acquisition phase.
Change the boot order to boot from the usb drive.
BIOS boots by reading the first sector on a hard drive, the boot sector code locates partitions with operating systems.

UEFI - boots by loading EFI program files.

Forensic boot tools: Paladin, kali, WinFE etc.
Forensic sorting tools: registryReport, ForensicUserInfo, FTK imager.

Forensic acquisition:

If not done properly data can be lost forever
It must be done in a way that does not invalidate it legally.

Information analysis layers on storage media:
- Physical: First to Last bit
- Volume: Only possible to recover volume information, no hidden areas ou unallocated sectors
- File: Only file information, less likely to retrieve deleted files.
- Application: Only app information on its own encoding.

The higher the acquisition layer, the less info is retrieved.

To copy storage media, you do it by blocks with the size of a sector, if any error exists it will only affect a block.
Should be at a physical level, to get hidden data.
Make either a forensic copy of the storage media, or read the data from the bios, normally not available.

On Post mortem boot a forensic tool and analyse the storage media
On alive systems, the os is running and can be used for data acquisition, but it might hide files.

Bad sectors -> Replace missing information with 0's and log the missing sectors.

Hidden areas: HPA and DCO

Write blockers and either Hardware or software, they act like a proxy and monitor all changes to the disk and block then.

To store acquired data:
- Cloning the data: from HD to HD
- Imaging the drive: from HD to iso

# Slide 4 Data Organization:

Data organization in layers:
- Layer 1: Physical level
- Layer 2: reading streams of 0's and 1's of RAM and disks
- Layer 3: File system
- Layer 4: Operating system and application level

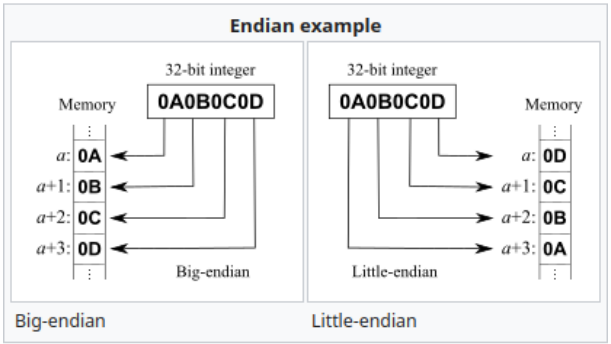
Analyse file system to:
- find files
- recover deleted files
- find hidden data

the result can be:
- file content
- data fragments
- metadata associated with files

Files data structure depends on the application that it was created, like HTML vs JPEG.

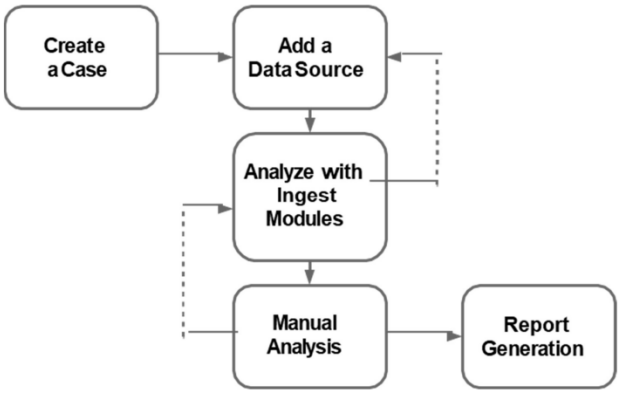
Big endian -> Most significant bit in lower storage address.

Little endian -> Less significant bit in lower storage address.




Data structures are placed continuously in memory.

## Slide 5 Autopsy:

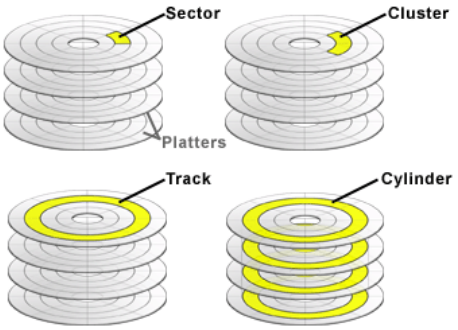



## Slide 6 Storage Devices:

Direct access: without bios, reading and writing directly through the hard disk controller

Access with Bios: slower, but simple as the bios communicate with the HD.

Hard disk Geometry:
- Tracks
- Cylinders
- Sectors




HPA (Host protected area): Special area to store vendor data, it does not erase with a format, located at the end of the disk and can be used to hide illegal files.

To recognize the HPA exists commands can show.

DCO (Device configuration overlay): Used to configure the capabilities of a disk, it can have more physical capabilities, but only the number on the DCO is

shown to the OS. Can be used to store hidden information. It can be removed but not created again.

SCSI and ATA are interfaces for communication that connect to hard drives.

NAND Flash memory:

HDD vs SSD:
- SSD has no mechanical parts
- Read speed is independent of location
- Less power consumption
- No vibrations

Flash Memory: type of medium used to store information with either nor gates or nand gates.

DRAM: volatile memory used in RAM

NOR Flash Memory: used for small amounts of memory with very fast readings and slow write/delete. Used in BIOS

NAND Flash Memory: large bit density, most used in the industry, is used in SSD and USB drives.

Inner working of a NAND chip:
- at rest =1 , at load =0

Minimum write and read units differ. Unlike a hard drive which is sector by sector.
Has garbage collection and a limited number of erasing cycles for each cell.
A cell is a single bit.
On a HDD you can write to a specific sector, on a ssd you can’t.

USB uses flash memory and is controlled by the processor.
SSD has its own processor, garbage collection starts as soon as it gets power.

## Slide 7 Volumes and Partitions:

Volumes: is a collection of sectors that at the physical level may not be consecutive, but for the OS they are consecutive, they are formatted in a specific file system (ext4, NTFS, etc.)

Partitions: Particular case of volumes where sectors are consecutive.

Volume structure must be identified to attempt to recover info, and can be used for separate files, dual boot etc.

Partition Tables: table that stores the information where the partitions start and end.

When the computer starts, the OS uses the Partition information (MBR ou GPT) to look for the partition with the boot flag, and run the bootloader.

LBA address: Address that maps to the physical sectors of the drive.

Procedure: read the partition table and identify layout.

Common partitions:

The MBR record is used by Microsoft mainly and contains boot code to process the partition table and find the OS. It's older and only allows for 4 primary partitions, with an extended one.

GPT is newer.

BSD is used by operating systems such as openBSD or freeBSD.

Volume aggregation:
- Used because it can improve performance and add redundancy.

Most Common: RAID (multiple versions) or spanning

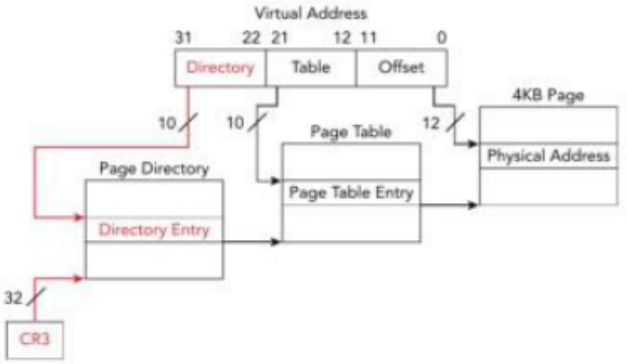
Raid can be implemented in hardware or software.

## Slide 8 RAM Analysis:

Information can only be available in RAM, and never written to the hard drive.

DMA: controls data transfers without the regulation of a CPU.

Paging: virtualize a linear address space.
each page has 4kB normally.
Forensic software must emulate the
virtual address space and handle the
virtual to physical address translation.




Memory acquisition: copy the contents from RAM to non-volatile storage.
Using a proper tool is important.

Software based memory acquisition:
- Remote or local
- Cost
- File format
- CLI or GUI
- Which part of the memory is needed.

There is risk associated with memory dumps, as it can corrupt an OS and lead to instability. On critical systems the consequences have to be measured.
This happens because data is always changing in RAM, caches must also be updated and there are parts of memory reserved for motherboard devices firmware that can not be altered.

Dump always to an external usb.

Most tools load a kernel module that maps the physical addresses to the virtual address space of a process, access the data and write it to non volatile memory.

## Slide 9 Mobile Forensics:

Smartphones have a huge potential to find evidence.

Data can exist in three locations:
- Handset, Memory card, SIM card

Data can also be in service providers, cloud services and handset backups

UICC: Physical part of the smart card (sim card)
SIM: Logical module stored inside the smart card

UICC has storage and a processor.

ICCID: Uniquely identifies the card.

Role of a SIM:
- Authentication (identification and authentication on network)
- Accountability (costs)

USIM: new type of SIM

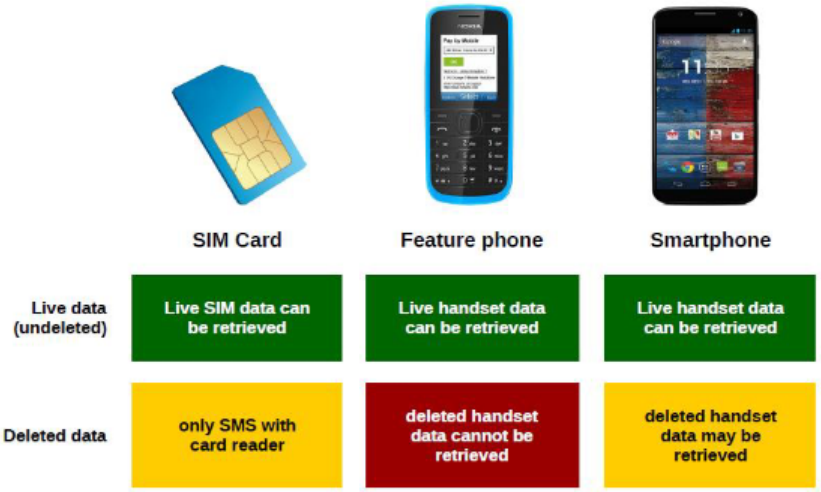
IMSI: identifies the subscriber and can not be altered or faked, and is not known.

MSISDN: phone number with the identifier of the country.

IMEI: identifies the phone.

When a sms is deleted from a (U)SIM, the message can stay in memory until a new one overwrites the space.
Network data can be used to get location information.

To ensure network isolation, use airplane mode or faraday cage.




Hashing every file instead of a single hash on the drive.

## Slide 10 Open Source INTelligence:

Information Sources:
Origin:
- Primary: original information
- Secondary: document or record that relates or dicuesses information of the primary source
- Tertiary: information source made up of lists of other information sources (Primary or Secondary)

Authority:
- Closed source: involves judicial authorization.
- Open source: fully accessible by third parties.

Advantages of Open Source:
- Less costly, easy access
- Does not compromise the investigation

Disadvantages of Open Source:

- Some information must be kept secret
- Can be arbitrary or misinformation

Information to Intelligence Cycle:

Levels: Strategic, Operational, Tactical, Technical

Skills of the analyst:
OSINT process:

1. Know who knows: in depth knowledge of available sources.
2. Know what's what: ability to evaluate and assess the validity, scope and accuracy of the requirements.
3. Know what's hot: important and relevant information
4. Know who's who: differentiate facts from speculation.

Open source possibilities:
- Traditional Media Sources
- Internet
- Public Data
- Professional and academic sources