Computer Forensics and Cyber Crime Analysis

Alessandro Milani

November 11, 2024

Contents

Part I

Legal

Chapter 1

Legal Introduction

Beafore the technology was between us (classic telephon call), but with the advanced of the information technology, the technology is now about us (facial recognition, social media, etc).
Example: The IA act say taht is not possible utilize IA for real time facial recognition without an "important" reason.
This generation use technology also for be profiled by an alghoritm for varius scope and not only for comunicate.

The "technology was between us" was simpler and the only problem was to cehck if there is a conversetion and intercept it with a good quality. Now, we have the problem of quantity. If we need to analyze data from milions of people we can end to vaiolate fundamental rights and make mistaks (even with OSINT).
Surovieky theory: collective intelligence, the point is that if you have 10k persons say that the restuarant is good and only 10 that say it's a froud, the collective intelligence say that the majority have right. In Forensics this can not be applied because you need to be 100% secure of what you have. (if in a trial you have only the 1% that a person can't be guily you need to be in favor of him) [find better term]

In the technology in Us, and the advance of IA is important that the law split waht is uman and what is not (like be transparent when a content is AI gen and when not)

"Tesla case" whan there is an incident it need to understand in the percent of error that is from tesla and the percent from the partners.

1.1 GDPR aand alghoritm bias

Art.22 of GDPR, say that you always need to have human in the decision process

1.2 Example - Lex Machina

Tool that analyze all the legal case from a giurisdiction (like France) and classify all the case in different categorys. So if you have a case X in Paris with judge Y, you have 60% possibility to win. If the Attorny ins Z, the probability is 80%.

1.3 Example - Compas

alghoritm that help the jugde defice is the person can commit other crime or not and so decide it need to stay in jail or get a reduce in the sentence (sconto della pena)

- A False positive in digital forensics can change people's lives.

Chapter 2

Foundations of Digital Forensics

2.1 Intro and definitions

2.1.1 Digital and Electronic Evidence

By the Scientific Working Group on Digital Evidence (**SWGDE**) a definition of, **digital evidence** is "any information of evidential value whether memorized or sent in a digital format". It's used by the **Council of Europe**
Another definition come from the **Eoghan Casey - 2004** that define a d**igital evidence or electronic evidence** as "any probative informationstored or transmitted in digital form that a party to a court case may use at trial". It's more related to the juridical part.
A last definition of **Electronic evidence** is information generated, stored or transmitted using electronic devices that may be relied upon in court, defined by the **Council of Europe - 2013**.

> For the exam, the first dfinition is the more important

So. in general, way we can say that a digital/electronic evidence need to be:

- **invisible** to the untrained eye
- Need to be **interpreted** by a specialist
- It may be **altered** or **destroyed** through normal use
- It can be **copied** without limits

Legal Requirements

The main characteristics that a Digital/Electronic Evidence need to have to be accepted in a trial are:

- **Admissability:** it need to be compliant with law and best practices.
  What can be seen is not what can be admissed in court (ex. if the italian police enter in a laptop, can only "wiretapping", by enabling mic and camera, and can't use other information like email or files in court)
- **Authenticity:** avoid any digital evidence tampering
- **Reliability and believability:** readily understandable for a judge.
  If a judge not understand the evidence can ignore it
- **Proportionality:** respect fundamental rights of parties affected by the measure

Find a digital evidence

A digital evicence can be hidden in different place and a criminal usully use some classical ways (not the cloud becasue the access is easy form a pocile force) like hidden folder, usb, extrnal memory etc.. can be hidden everywhere

Categories

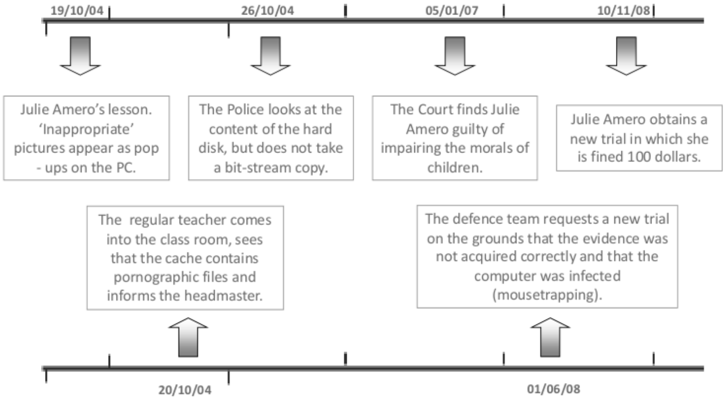
Three main types of digital evidence

- **Created by human**: digital data result of an action taken by an human
  - *Human to Human*: Like an email
  - *Human to PC*: like a word document
- **Created indipendenlty by the computer**: data that are result of the processing of data by an algorithm and without human intervention
- **Created by both human and the computer**: somethings like a spreadsheet where the data are entered by the human, and the result is worked out by the computer

Julie Amero Case

> This case is not import for the exam

Julie Amero is a supply teacher at Kelly School in Norwich, Connecticut who was found guilty of showing pornography to children under the age of 16 for some popup that appear during a lesson



Julie Amero's lesson. 'Inappropriate' pictures appear as pop - ups on the PC.

The Police looks at the content of the hard disk, but does not take a bit-stream copy.

The Court finds Julie Amero guilty of impairing the morals of children.

Julie Amero obtains a new trial in which she is fined 100 dollars.

The regular teacher comes into the class room, sees that the cache contains pornographic files and informs the headmaster.

The defence team requests a new trial on the grounds that the evidence was not acquired correctly and that the computer was infected (mousetrapping).

Figure 2.1: Timeline of the case

2.1.2 What is digital Forensics

Digital Forensics is get hold of evidence without modifing the IT system in which that evidence is found, ensure that the evicence acuired in another medium is identical to the original and analyse data without modifyin it.

2.1.3 The “Big Five” of Digital Forensics (Council of Europe)

- **Data Integrity:** No action taken *should change electronic devices or media*, which may subsequently be relied upon in court.
- **Chain of custody:** An *audit trail* of all actions taken when handling electronic evidence should be created and preserved
- **Specialist Support:** If investigations involving search and seizure of electronic evidence it may be necessary to consult *external specialists.*
- **Appropriate Training:** First responders *must be appropriately trained* to be able to search for and seize electronic evidence if no experts are available at the scene
- **Legality:** The person and agency in charge of the case are responsible for ensuring that *the law and the above listed principles* are adhered to.

2.2 Digital Forensics Procedure

Six phase of digital forensics procedure:

2.2.1 Identify the Suspect

There are 3 main phase for identify the suspect:

- **Osint and Socmint:** Very usefull for collect information reguarding criminal (even mafia ones), from social media, and other public sources.
- **Data Retension Directive in EU:** The investigator uses the Court System to compel the ISP to reveal a physical location that corresponds likely to the source of Network (IP Address)
- **Multiple User ID or multiple Ips over time, open Wi-Fi, Proxy, Botnet**: Under a warrant (depending from the Jurisdiction) the location is searched and any computer or other device is seized

Data Retension

With the Directive 2006/24/EC, the EU member states are required to store data for a period of **6 to 24 months** (but can change from state to state). The data stored are gerally call detail records (CDR) of telephony and internet traffic and location data (IPDRs).
So evert single country and ISP have different data retention policy, and this can be a problem for the investigator, but from a privacy point of view a short time or null data retention is better.

Transparency report: Every year the ISP need to publish a transparency report where they show the number of request of data retention and the number of request that they have accepted.

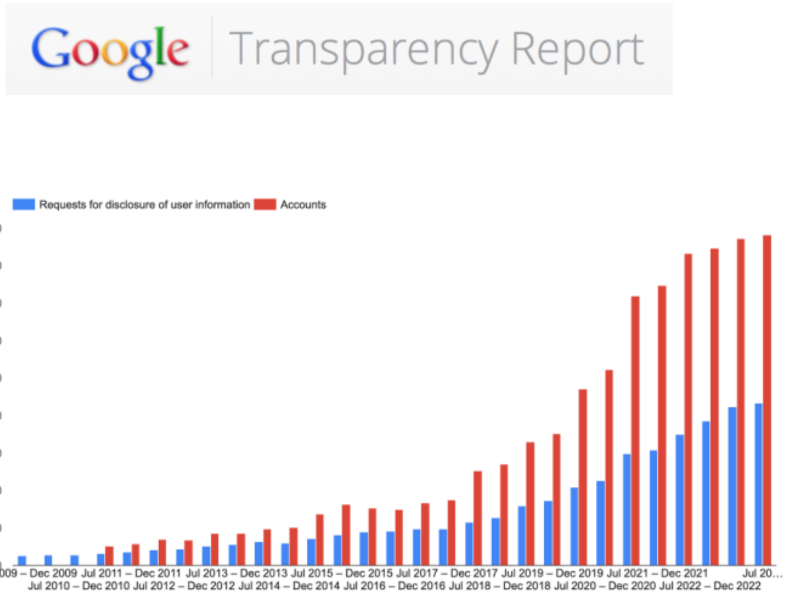


Figure 2.2: Timeline of Google transparency report

Identify the suspect

it's rigth use face recognision to identify a suspect?
For the moment if the situation is critical is possible utiliza A live facial recognision.
AI act also regulate the use of facial recognision.

2.2.2 Detecting and Seizing Digital Evidence

The seize of digital evicences has torespet two foundamental rules: **bit-Stram Copy** and **Hash Function**. (definitions are alredy knowed)

Where and how is the digital/electronic evidence hosted?

The digital evicence can be in the suspected PC or in a third party server.
In the first case, we need to mange the encrition of the data, and it's possible get a Key Mandatory Law.
In the case of evicende in a server, is needed a collaborationfrom the ISP/Telco/Banck, and so need there is Jurisdiction problem.

The role of third paries during digital investigation

A third party can give a lot of usefull information.
For example and **ISP** Could reveal from which place the email was sent, the **Mail Account Provider** could reveal from which places the email account was accessed and a **Credit Card Company** could reveal where the goods bought with a cloned credit card were delivered

2.2.3 Validating Digital Evidence

There is some tool that help to valdiate online digital evidence.
These kind of tool are usefull during OSINT bacasue they permit to collect data (like a story, a reel), that are not sure remain online, in a proper way for a court.

2.2.4 Chain of Custody

Digital storage media last less than analogue media and devices to read such media last even less. For example a LaserDisc last only 15 years, where there are books form thr 1086 (domesday book). So there at the moment, for trial, there are a lot of hard drive keeped in proprer way to avoid the data loss. It's a real mess.

2.2.5 Analysis of Digital Evidence

Start after the sieze of suspect's device, and need to be performed besided a precise chain of custody.
To perform the analysis are usually used some automatic tools, but in the recent time are used also some AI tools but only for post analysis and not for prediction policies (limitation imposed by the AI act) for example AI can not be used for kidnapping cases because the crime is in progress and not "finished".

- **Text searches:** aimed at scanning files, directories and even entire file systems for specific text terms (generative AI can be used for summarizing and analyzing documents, but it's not very precise, plus alucination)
- **Image searches:** aimed at identifying image files in various formats, and at generating still frames of digitally stored video footage. Mainly analysis of child pornography that can be lead also to false positive (like a video of a mum and child in a bath)
- **Data recovery:** aimed at recovering all files stored on mass memory units, including deleted or damaged data. Destroy data can also be a crime (even if there are some backups), based on the intention of the crime (like delete file to hide evidence)
- **Data discovery:** targeted at accessing hidden, encrypted or otherwise protected data
- **Data carving:** focused on reconstructing damaged files by retrieving portions of their content
- **Metadata recovery and identification:** this digital forensic tool is particularly useful for retracing the timeline of web accesses and file changes

Some other problem withthe use of **AI for prediction** of crime are: the bias of the AI and possible conseguences for privacy and **social control** by not very democratic government.

Two Italian issues

Repeatable or Unrepeatable forensics analysis: **Repetable** when you can do a bit-stream copy of the data and also give one copy to the defence to do the same analysis, and more in general i can repeat analysis again and again (when i want).
In a **non-repetable** analysis, we need do live forensics activity and ofter occure with mobile phone, where there isn't the possibility to do a bit-stream copy of the data. In the live forensics i also need the presence of the attorney or the defender when i do the analysis to make it admissable in court.

Open Source or Closed Source: Open source can be more transparent

2.2.6 Presentation in Court

The presentation of digital evidence findings is a **crucial stage** for prosecutors, judges, and lawyers (the evidence need to be presented in a way that the judge can understand it otherwire he can ignor it). The outcome of the trial relies not only on the results of the investigation but also on the **clarity and comprehensibility** of the report provided.

Operational Recommendations:

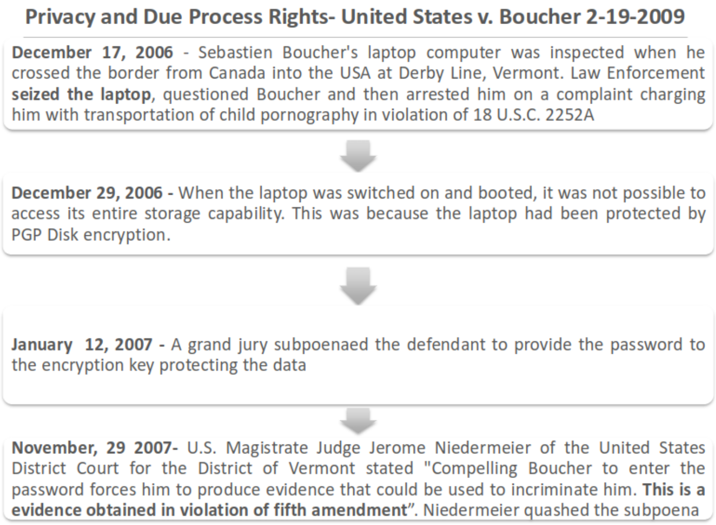
- **Presence of an index:** The report should include a clear index for easy navigation through the document.
- **Glossary and Reference Notes:** If technical terms are used, a glossary and reference notes should be provided to ensure that all parties understand the terminology (judge and lawyers are not IT experts).
- **Timeline Table and Flow Charts:** A timeline table or flow charts should be included to visually represent the sequence of events and digital activities.
- **Presentation Slides with Photos:** Visual aids, such as presentation slides with photos, help in simplifying complex technical details.
- **Video Recording:** Where applicable, video recordings of the operations carried out during the investigation can provide further clarity.

Presentation in Court of the Digital Evidence Findings: Murtha Case

2.3 Privacy and Due Process Rights

2.3.1 Encryption

Encryption can be used to hide the fact that encrypted messages are exchanged and used by criminals can lead to difficulties collecting the necessary evidence



Privacy and Due Process Rights- United States v. Boucher 2-19-2009

December 17, 2006 - Sebastien Boucher's laptop computer was inspected when he crossed the border from Canada into the USA at Derby Line, Vermont. Law Enforcement **seized the laptop**, questioned Boucher and then arrested him on a complaint charging him with transportation of child pornography in violation of 18 U.S.C. 2252A

December 29, 2006 - When the laptop was switched on and booted, it was not possible to access its entire storage capability. This was because the laptop had been protected by PGP Disk encryption.

January 12, 2007 - A grand jury subpoenaed the defendant to provide the password to the encryption key protecting the data

November, 29 2007- U.S. Magistrate Judge Jerome Niedermeier of the United States District Court for the District of Vermont stated "Compelling Boucher to enter the password forces him to produce evidence that could be used to incriminate him. **This is a evidence obtained in violation of fifth amendment**". Niedermeier quashed the subpoena

Figure 2.3: Case correlated with the use of encryption

2.3.2 Case Law on Encryption

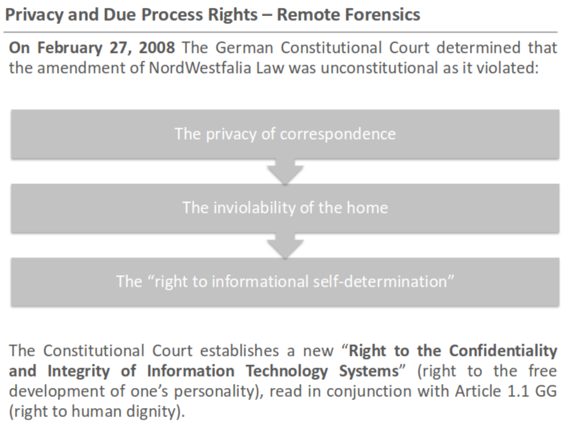
Anther the previus case, some state are starting to create law about “Mandatory Key Disclosure” that force the suspect to give the key/password to decrypt the data. (some are Australia, Belgium France etc. . .)

2.3.3 Mandatory Key Disclosure Laws

These case of legislative instrument doesn’t work fow two main reason:

- **technical reason:** An expert could always find a way yo hide a file
- **Possible violation of European Convention on Human Rights:** Article 6 Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law

2.3.4 Remote Forensics



Privacy and Due Process Rights – Remote Forensics

On February 27, 2008 The German Constitutional Court determined that the amendment of NordWestfalia Law was unconstitutional as it violated:

The privacy of correspondence
The inviolability of the home
The “right to informational self-determination”

The Constitutional Court establishes a new “**Right to the Confidentiality and Integrity of Information Technology Systems**” (right to the free development of one’s personality), read in conjunction with Article 1.1 GG (right to human dignity).

Figure 2.4: Case correlated to remote forensics

2.3.5 Cloud Computing

Cloud computing services face two key legal challenges: **Jurisdiction** and **Privacy**.

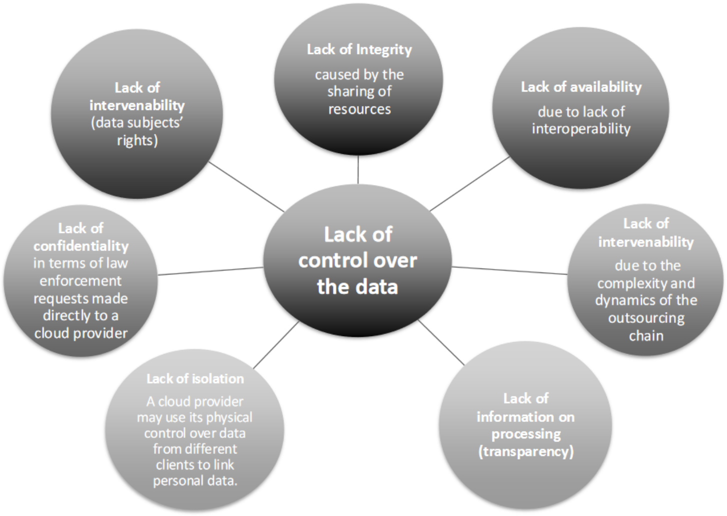
Jurisdiction The “**loss of location**” of digital evidence in the cloud introduces significant jurisdictional issues. In a cloud environment, the question arises: are the documents governed by the laws of the state in which they are physically located, the location of the company possessing them, or the laws of the state where the individual resides?

Over the last few years, various legal frameworks and approaches have been proposed to address this complex issue, but it remains an area of ongoing debate.

Privacy Cloud computing introduces several privacy concerns, including:

- **Lack of Control:** Cloud clients may no longer maintain exclusive control over their data, limiting their ability to implement necessary technical and organizational measures to comply with **Data Protection Laws**.
- **Absence of Transparency:** Cloud providers may not provide sufficient information regarding how data is processed, leading to significant risks in terms of compliance with data protection regulations.

Lack of control over the data


Lack of control over the data
Lack of intervenability (data subjects' rights)
Lack of Integrity caused by the sharing of resources
Lack of availability due to lack of interoperability
Lack of confidentiality in terms of law enforcement requests made directly to a cloud provider
Lack of intervenability due to the complexity and dynamics of the outsourcing chain
Lack of isolation A cloud provider may use its physical control over data from different clients to link personal data.
Lack of information on processing (transparency)

Jurisdiction

In addressing the "loss of location" issue within the realm of cloud computing, we have four possible legal principles that can be applied:

- **Territorial Principle:** The court in the jurisdiction where the data is physically located has authority. Jurisdiction is determined based on the geographical location of the data.
- **Nationality Principle:** The nationality of the perpetrator is used to establish criminal jurisdiction. The legal framework of the country of the individual committing the crime applies.
- **Flag Principle:** This principle applies to crimes committed on ships, aircraft, and spacecraft. They are subject to the jurisdiction of the country whose flag the vehicle flies under.
- **Power of Disposal Approach:** This approach focuses on who has control over the data. A regulation based on this would enable law enforcement to access a suspect's data in the cloud, regardless of its physical location, by considering the individual or entity with power over the data.

Chapter 3

Convention on Cybercrime

3.1 E-commerce on Dark Web

The Dark Web provides a platform for buyers and sellers to engage in e-commerce transactions, often involving illicit goods and services. This anonymous marketplace operates with the same principles as traditional e-commerce, but with heightened security and privacy measures to conceal identities.
Vendors on the Dark Web offer a wide range of products, from drugs and weapons to stolen data and hacking services. Buyers can browse listings, read reviews, and complete purchases using cryptocurrencies, all while maintaining a high degree of anonymity.

3.1.1 Silk Road

Silk Road, often referred to as the "eBay of drugs," was an online marketplace that facilitated the sale of a wide range of illegal substances, including narcotics and controlled substances. At its peak in 2013, Silk Road had a reported annual revenue of $89.7 million

- **Combining Tor, PGP, and Bitcoin**: Ross Ulbricht leveraged the anonymity of Tor, the encryption of PGP, and the decentralized nature of Bitcoin to create the Silk Road marketplace.
- **Bitcoin-only Payments**: Silk Road required all transactions to be conducted using Bitcoin, providing an added layer of anonymity and making it harder to trace purchases.
- **User-friendly Interface**: Silk Road featured a well-designed interface that allowed users to easily navigate the site and leave feedback on their transactions.
- **Intermediary Role:** Silk Road acted as an intermediary, handling the payment processing nad logistics of shipping items purchased on the marketplace.

Silk Road Investigations

- **Operation "Marco Polo":** Undercover agents from DEA and Secret Service involved in exorting money from Ulbricht and attempting to threaten him.
- **Silk Road's Scpoe:** At its peck:
  - 950,000 registered users
  - 1.2 million transactions
  - $79 million in commissions
- **Incriminating Errors:** Ulbricht made several mistakes that led to his arrest, including using his real email address and have counterfeit documents delivered to his home.

Charges Against Ross Ulbricht

- **SUmmary of Charges:** Ulbricht faced 7 key charges, including drug trafficking, money laundering, and computer hacking, which were consolidated into 3 main counts against him
- **Legal Process:** The trial lasted just 13 days and resulted in Ulbricht's conviction and life sentence, plus $180 million in damages

The investigation was possible because involve US citizen, US platform, and US law enforcement. In another country, the same investigation would have been more difficult.

3.2 History and objectives of the Convention on Cybercrime (Budapest Convention)

The convention involve 65+ states, and its main objectives are:

- Harmonizing national laws on cybercrime
- Improving investigative techniques
- Increasing international cooperation

3.2.1 Overview of the Convention

Timeline and Ratification

> The Council of Europe ≠ Europe Union, and it's composed by state that are part of the European continent, and its conventions are open to non-European countries.

- Full Adoption: Committee of Ministers of the Council of Europe, November 8, 2001
- Signature: Budapest, November 23, 2001
- Entry into Force: July 1, 2004
- Participating States (as of April 2023):
  - 68 States have ratified
  - 2 States signed but not ratified (Ireland, South Africa), so for them is not binding

Criticism and Opposition

- **India:** Initially refused to adopt due to non-participation in drafting
- **Reconsideration** (since 2018): Surge in cybercrime, but concerns about data sharing with foreign agencies remain
- **Russia**: Rejected due to concerns about sovereignty, limited cooperation in international investigations, even after some articles were revised to address these concerns

New Global Cybercrime Treaty (UN, August 8, 2024)

Content:

- Criminalization of unauthorized access to information systems
- Crimes related to online child exploitation and non- consensual explicit content distribution

Criticism

- Concerns over human rights and press freedom
- Issues with data privacy and overly broad definitions of cybercrime

3.2.2 Aim of the Convention

The convention aims to assist in combating crimes that are inherently linked to the use of technology, where devices serve as both the tool for committing the crime and the target of the crime

> **Note:** there are differences when a crime is commited through a technology tool, and when the technology is the target of the crime.

as well as crimes where technology is used to enhance other criminal activities, such as fraud. It provides guidelines for countries to develop domestic cybercrime laws and acts as a foundation for international cooperation between parties.
The **first additional protocol** focuses on criminalizing the dissemination of racist and xenophobic material through computer systems, along with threats and insults motivated by racism and xenophobia.
The **second additional protocol** establishes common international rules to enhance cooperation on cybercrime, particularly in the collection of electronic evidence for criminal investigations and proceedings.

3.2.3 Key points

Original Convention (1 July 2004)

- The convention covers:
  - The criminalisation of conduct: ranging from illegal access, data and systems interference to computer-related fraud and dissemination of child abuse material;
  - Procedural powers to investigate cybercrime and secure electronic evidence in relation to any crime;
  - Efficient international cooperation between parties.
- Parties are members of the Cybercrime Convention Committee and share information and experience, assess implementation of the convention or interpret the convention through guidance notes.
- Of the 27 Member States, 26 have ratified the convention - Ireland has signed but not yet ratified it.

Additional Protocol 1 (1 March 2006)

This protocol extends the scope of the convention to cover xenophobic and racist propaganda disseminated through computer systems, providing more protection for victims. It furthermore:

- Reinforces the legal framework through a set of guidelines for criminalising xenophobia and racist propaganda in cyberspace;
- Enhances the ways and means for international cooperation in the investigation and prosecution of racist and xenophobic crimes online.

Additional Protocol 2 (8 August 2024)

This protocol aims to further enhance international cooperation.
It addresses the particular challenge of electronic evidence relating to cybercrime and other offences being held by service providers in foreign jurisdictions, but with law enforcement powers limited to national boundaries. Its main features are:

- A new legal basis permitting a direct request to registrars in other jurisdictions to obtain domain name registration information
- A new legal base permitting direct orders to service providers in other jurisdictions to obtain subscriber information
- Enhanced means for obtaining subscriber information and traffic data through "government to government" cooperation
- Expedited cooperation in emergency situations including the use of joint investigation teams and joint investigations. Key points of the Additional Protocol 2 (8 August 2024)

3.3 Harmonization of national laws and international cooperation

3.3.1 Internetional Cooperation Provisions

- **Coooperation Principle:** Parties are to cooperate "to the widest extent possible" in investigating electronic evidence.
- **Expedited Mutual Assistance:** Issue with Current Mechanisms: Mutual assistance requests are often slow and take months.
- **Convention solution:** Allows for expedited requests using "expedited means of communication" and Expedited means must provide adequate levels of security and authentication. (So can be used encrypted physical device for data transfer)
- **Voluntary Information Sharing:** Parties may share information without a formal request if it would assist in investigations or help the receiving party with any related offences.

3.3.2 Mutual Assistance Provisions

- **Procedural Powers for Assistance:**
  - Expedited Preservation of stored computer data.
  - Expedited Disclosure of traffic data.
  - Real-time Collection of traffic data and interception of content data: parties provide assistance according to domestic laws and applicable treaties, subject to any reservations.
- **Art 23 - General Cooperation Principle:**
  - Mutual assistance "to the widest extent possible" for:
  - Cyber-related offences.
  - Collection of electronic evidence for any criminal offence.
- **Restrictions:**
  - Cooperation may be restricted in cases of:

  - Extradition.
  - Mutual assistance regarding real-time collection of traffic data.
  - Interception of content data

3.3.3 24/7 Network for Immediate Assistance

Provision for Constant Availability:

- Each party must designate a contact point available 24/7
- Purpose: Provide immediate assistance for cybercrime investigations, proceedings, or the collection of electronic evidence
- Based on the G8 network of contact points model

Significance: aims to expedite the processing of urgent mutual assistance requests, overcoming current delays in traditional bureaucratic channels

3.4 Legal measures against computer-related fraud and forgery

3.4.1 Criminalization of Fraud and Computer-related Forgery

The Convention requires State Parties to criminalize specific conducts, including fraud and forgery carried out through computer systems. This includes, for instance, digital document forgery and fraud involving the use of electronic data to deceive or gain financial benefits.
Computer-related fraud involves using computers to gain economic benefits through deceit, while **forgery includes altering or creating digital documents** with the intent to mislead.

Computer-Related Forgery

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, **alteration**, **deletion**, or s**uppression of computer data**, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.
This kind of alteration it's often seen as less grave compared to the forgery fo a physical document, becasue at a cercain level is easier to do (like copy the image of a firm on a document).

Computer-Related Fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

- any input, alteration, deletion or suppression of computer data,
- any interference with the functioning of a computer system

With fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

3.4.2 Procedural Law Tools

To effectively address these crimes, the Convention introduces procedural law tools that allow for quicker and more effective investigations. For example, **expedited preservation of volatile data** and **seizure of information** are crucial tools for gathering evidence in investigations against digital fraud and forgery. The Convention mandates that criminal justice authorities must be able to use effective means, such as:

- *Search and seizure*
- *Access to stored data in computer systems*

These tools must be applicable regardless of the type of crime involved.

3.5 Procedural powers for law enforcement

3.5.1 Synopticon and Omnipticon

A **synoption** world, the many watch the few, so there is possibility to control the information, but in the digital world, in a **omnipticon** world, the many watch the many, so tit's extremly complex try to control the information.
The tv, as a synoption point of view have also keep the role of an "official information soruce", but in the last years, with the diffusion in the use of youtube or similar platform, also this role is starting to crumble.
In this new scenario, we need to consider how is a mess, from a legal stand point manage all the video.

> The **Main Concert** for private citizens and public administration using cloud techmologies is not so much the possibile increase in "cyber" fraud or crime, than the loss of control over one's data, for privacy reason and **digital investigaion purposes**

3.5.2 Some articles

> Articles from 14 to 20 are not very important for the Exam

Scope of Procedural Provisions (Article 14)

Each Party must adopt **legislative measures** to define the *powers and procedures* for specific criminal investigations or proceedings.
The provisions apply to:

- Offenses covered by the Convention,
- All other offenses committed through **computer systems**,
- All **electronic evidence** related to any crime.

Conditions and Safeguards (Article 15)

The application of **powers and procedures** must ensure *adequate protection of human rights*, following national law and international conventions (e.g., the **European Convention on Human Rights**). Conditions and safeguards include:

- **Judicial or independent supervision**,
- Consideration of *proportionality*,
- Protection of the *rights of third parties*.

3.5.3 Expedited Preservation of Stored Data (Article 16)

Authorities must be able to **order or obtain the rapid preservation** of specific computer data, particularly if there is reason to believe that the data is vulnerable to *deletion or modification*. This order may require the data's custodian to preserve the data for up to **90 days**, which is extendable as needed.
In Italy the authorities can access the list of the web access of the previus 5 years of a person if it's under investigation.

Expedited Disclosure of Traffic Data (Article 17)

To ensure data preservation, authorities can demand rapid disclosure of traffic data to identify service providers and communication pathways, even if multiple providers are involved in the transmission.

Production Order (Article 18)

Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

1. A person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium;
2. A service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

Subscriber Information (Article 18)

For the purpose of this article, the term *subscriber information* means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

1. The type of communication service used, the technical provisions taken there to, and the period of service;
2. The subscriber's identity, postal or geographic address, telephone and other access numbers, billing and payment information, available on the basis of the service agreement or arrangement;
3. Any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Search and Seizure of Stored Computer Data (Article 19)

> One of the least applicated article.

Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

1. A computer system or part of it and computer data stored therein; and
2. A computer-data storage medium in which computer data may be stored in its territory.

Real-time Collection of Traffic Data (Article 20)

Authorities can **collect** or record **traffic data in real time**, either directly or by requiring service providers to assist in the collection. (convention is usually limited to telco and ISP of the country)

Interception of Content Data (Article 21)

For serious offenses, **authorities may intercept or record the content of specific communications in real time**, either directly or through the cooperation of service providers.

Mutual Assistance (Article 25)

The Parties shall afford one another **mutual assistance to the widest extent possible for the purpose of investigations or proceedings** concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

Expedited Preservation of Stored Computer Data (Article 29)

A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.

Expedited Disclosure of Preserved Traffic Data (Article 30)

Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.

3.5.4 Article 32. Solution to Russia Concerns

A party may, without the authorisatoin of another Party:

- Acces publicy available stored computer data, regardless of where the data is located geographically
- Access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system

Conseguences of Article 32b

> LEAs routinely requestand are provided with data from from foreign service providers, withoutformal inter-State process such as mutual legal assistance (MLA). Ebay and Facebook hace dedicated portals for facilitating such Exhcaneges.

There are 5 proposed implementation from the Council of Europe for the article 32b:

1. ”Transborder access with consent without the limitation to data stored ’in another Party’”
2. ”Transborder access without consent but with lawfully obtained credentials”
3. ”Transborder access without consent in good faith or in exigent or other circumstances”
4. ”When the data is lawfully accessible or available from the initial system™
5. If the location of the data is not known, but the person having the power of disposal of the data is physically on the territory of, or a national of the searching Party, the LEA of this Party may be able [to] search or otherwise access the data

3.6 Some additional Legal framework

> An **EU regulation** is someting that is directly applicable in all the EU member states, so it's not necessary to be trasposed in the national law of the member states.

- **Regulation (EU) 2023/1543** of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal
  Text of the Regulation
- **Directive (EU) 2023/1544** of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings
  Text of the Directive

> An **EU directive** is a legal act that sets out a goal that all EU countries must achieve. However, it is up to the individual countries to devise their own laws on how to reach these goals. (the directive 2023/1544 must be trasposed in the national law by 18 February 2026)

Chapter 4

Italian Law n. 48/2008

4.1 Overview and Significance of Italian Law n. 48/2008 in the Context of Cybercrime in Italy

The Budapest Convention on Cybercrime was issued by the Council of Europe on November 23, 2001. Italy ratified the Convention with Law n. 48, after 7 years, on March 18 2008, which was published in the Official Gazette on April 4, 2008. But not all the principles presnet in the convention went conveted to law.

4.1.1 Budapest Convention on Cybercrime - Overview

The ratification of the Budapest Convention by Italy through Law n. 48/2008 represents a critical step in modernizing the Italian legal system to tackle cybercrime. This law aims to harmonize legal standards across borders, emphasizing the importance of international cooperation in addressing the rapidly evolving digital landscape. However, challenges remain in adapting to rapid technological changes, and continuous updates to legislative tools are necessary.

4.2 Main Innovations Introduced

- **International harmonization of legislations:** aligning laws internationally to combat cybercrime
- **Reorganization of cybercrime offenses:** amendments and integrations to the penal code, introducing new specific offenses
- **Corporate Liability:** extending the liability under Legislative Decree 231/2001 to cover certain cybercrime offenses

4.2.1 Corporate Criminal Liability

The law extends corporate criminal liability for offenses committed in the interest or for the benefit of the company, as regulated by Legislative Decree 231/2001. This applies to all legal entities, even foreign companies if the offense is committed in Italy, for the interest or for the benefit of the company. The liability extends to offenses such as:

When the offence is committed by:

- **Persons holding a position of representation**, management or direction or who exercise, even if de facto, management and control (”Top Management”)
- **Persons subject to the control** or monitoring activity of the Top Management.

> So there are 2 trials that procede in parallel, one for the company and one for the individual. And if it's proved that the action was done in the interest of the company, the company is liable.

- Crimes against public administration
- Tax offenses
- Money laundering / receiving stolen goods
- Organized crime offenses
- Computer crimes
- "Corporate" offenses (including private to private corruption)

> The company over the traditional defence could demostrate that have a compliance program in place, so a series of policies that are designed to prevent the commission of crimes, and the employee have broke them. Are often called **Soft Law**

There aren't poilices for avoid all the crimes, but if an employee commit a crime, without break the company policies, the company can can avoid the liability if the policies are recognize as valid ("the employee is too good").

4.2.2 Further Innovations

Additional measures introduced include:

- Establishment of a fund under the Ministry of the Interior to combat child pornography online.
- Updates to data retention laws with reference to Directive 2006/24/EC.
- Enhancement of international cooperation, especially concerning mutual assistance in cybercrime investigations.
- Acquisition of digital evidence: Updates to criminal procedure code for regulating the collection and use of digital evidence.

4.3 Key Provisions and Their Implications for Digital Forensics

4.3.1 Major Procedural and Investigative Updates

International Cooperation

The law enables the Ministry of the Interior or designated authorities to instruct internet and telecommunications providers to retain and protect traffic data for up to 90 days. This period can be extended to six months for specific investigative needs, but excludes the content of communications.

Competence for Investigations and Prosecutions

Cybercrime investigations and prosecutions are assigned to the Public Prosecutor's Office at the Court of Appeal's main district. This aims to improve coordination in cybercrime cases. However, initial issues arose due to the lack of transitional provisions for ongoing investigations, which were later addressed by Law n. 125 of July 2008.

Service Providers' Role

Service providers, including internet, telecommunications, and postal services, play a key role in combating cybercrime. Their responsibilities include:

- Retention of traffic data and communication logs.
- Seizure of correspondence, including electronic communications, when linked to criminal investigations.
- Seizure of digital data, ensuring that original data is preserved while copies are made without modification.

Legal Recognition of Computer Forensics

The law introduces computer forensics as a significant element of investigative practices, with clear protocols for handling digital evidence. These practices will need continuous updates as technology evolves.

4.3.2 Best Practices in Digital Evidence Handling

The law advocates for "best practices" in digital evidence handling, emphasizing the importance of:

- Acquiring evidence without altering the original device.
- Authenticating both the evidence and its digital copy.
- Ensuring that the examination process is repeatable.
- Maintaining impartiality in technical analysis.

4.3.3 Email Seizures

The law also includes provisions for seizing email communications, granting the same legal protections to both traditional and electronic mail.

4.3.4 Changes to the Code of Criminal Procedure

The law modifies the Code of Criminal Procedure to extend investigative measures such as inspections and seizures to digital environments. Noteworthy amendments include:

- **Digital Inspections and Searches:** Technical measures must be implemented to preserve the integrity of the original data and avoid alterations.
- **Preservation Orders (Freezing):** These orders are introduced as a quick measure to secure digital evidence before it can be lost or tampered with.

4.4 Law n. 48/2008: Areas for Improvement

4.4.1 Standardization of Digital Evidence Procedures

Law n. 48/2008 established a unified approach for handling digital evidence in criminal proceedings. This standardization focuses on the acquisition, preservation, and presentation of digital evidence, ensuring its integrity and authenticity for admissibility in court.

4.4.2 Judicial Expertise and Training in Digital Forensics

The implementation of this law has increased the responsibility of legal professionals to understand digital forensics. There is a growing need for specialized training in this area to avoid misinterpretation of digital evidence.

4.4.3 Legal Certainty and Data Integrity

Ensuring the integrity and authenticity of digital data is crucial. Law n. 48/2008 improved the reliability of digital evidence in court by requiring that data remain unaltered during acquisition and preservation. However, further refinement of these procedures is necessary, especially with the rise of more sophisticated cyber threats.

4.5 Case Studies and Practical Applications of Italian Law n. 48/2008

4.5.1 Case Study 1: Data Seizure and Service Providers

Phishing cases often involve the seizure of data from service providers to trace illegal transactions. Although no specific case is named, this method is frequently used in investigations of fraud and financial crimes.

4.5.2 Case Study 2: Organized Crime and Communication Monitoring

A significant case involved intercepting communications of mafia organizations in Italy. This was part of a broader initiative coordinated with Europol and Interpol, utilizing advanced digital forensic techniques to collect evidence from encrypted messages.

4.5.3 Case Study 3: Cyberstalking

In several cyberstalking cases in Italy, digital forensics were employed to trace online threats' origins. Investigators successfully identified offenders through data traffic analysis and IP identification, making this a common approach in Italian jurisprudence.

4.6 Types of Corporate Investigations

- **Unfair Competition:** Investigating unethical practices by rival businesses.
- **Industrial Espionage:** Uncovering the theft of trade secrets and proprietary information.
- **Employee Misconduct:** Addressing violations of company policies and contracts.
- **Intellectual Property Infringement:** Protecting copyrights, trademarks, and patents from unauthorized use.

4.7 Man-in-the-Middle (MITM) Attacks

MITM attacks represent a silent and sophisticated form of cybercrime where an attacker intercepts communication between two parties. This allows criminals to monitor, read, and modify messages undetected, often targeting businesses involved in international trade.

The attack's success relies on the attacker's ability to remain undetected while gathering crucial information **over an extended period**.

4.7.1 The Mechanics of MITM Attacks

- **Initial Breach:** Hackers compromise a company's email system through methods such as phishing, brute force attacks, or trojans.
- **Monitoring Phase:** Attackers observe communications over time, gathering information on business practices and relationships.
- **Interception:** At an opportune moment, criminals intercept and alter payment instructions, redirecting funds to their accounts. When one party requests a payment, the attacker sends fraudulent account details to the other party (like by editing the mail with the invoice).
- **Execution:** Unaware of the fraud, victims transfer funds to the fraudulent account, often resulting in significant financial loss.

4.7.2 Legal Implications of MITM Attacks

Criminal Perspective: MITM attacks can be classified as fraud under Article 640 of the Italian Criminal Code, involving deception through false emails and documents. **Identity Theft:** Such attacks may also fall under identity substitution (Article 494) and computer fraud (Article 640 ter), particularly with recent legislative changes.

Jurisdictional Challenges

Prosecution of MITM attacks is often complicated by jurisdictional issues and time constraints, as attackers frequently operate from countries with limited judicial cooperation.

4.7.3 Civil Recourse and Bank Responsibilities

Immediate Action: Victims should promptly request payment reversals while funds remain in the destination account. Some European banks may assist by freezing accounts and returning funds.

Bank Liability: European regulations, such as the Payment Service Regulation and Italian Legislative Decree 27 January 2010, n. 11, often shield banks from liability, even when account holder details do not match.

Regulatory Gaps: Current regulations may be insufficient in an era of fast online payments, where financial intermediaries predominantly control transaction verification.

Chapter 5

UN Resolution on Cybercrime

5.1 Background and Objectives of the Resolution

The primary objective of this resolution is to initiate the drafting of a global treaty aimed at combating cybercrime through multilateral negotiations. The title, "Countering the use of information and communications technologies for criminal purposes," signifies a step towards developing an international convention on cybercrime, targeting the implementation of concrete measures against this form of crime.

The resolution establishes a dedicated Committee responsible for drafting a comprehensive convention. This process is expected to be transparent, involving a wide range of stakeholders, such as developing countries, intergovernmental organizations, and field experts.

5.2 Impact on International Cybersecurity Policies and Practices

5.2.1 UN Resolution (26 May 2021)

This resolution could significantly impact international cybersecurity policies, promoting greater cooperation and harmonization among states. By establishing shared minimum standards through an international cybercrime treaty, it fosters a more unified regulatory framework and enhances investigative cooperation across different jurisdictions.

The adoption of the resolution required various amendments and compromises, highlighting the importance of balancing national and supranational interests while ensuring inclusivity and transparency.

5.2.2 Human Rights and Privacy Risks

One of the central issues discussed in the UN report is the need to balance cybersecurity measures with the protection of human rights, particularly privacy and data protection. Although there is a consensus on the importance of cybersecurity, the UN GGE report warns against overreach, as unregulated measures may infringe on civil liberties.

5.2.3 Emerging Threats and Supply Chain Integrity

The report emphasizes the growing risks associated with vulnerabilities in global supply chains, especially in the ICT sector. Such vulnerabilities could lead to large-scale attacks or espionage, underlining the need for states to secure digital infrastructures and collaborate on emerging threat information.

5.3 Future Legal Framework for Cybersecurity

Cybersecurity policymakers are required to implement stringent measures to protect data during investigations. Legislative provisions should allow for periodic review and updates to cybersecurity practices, ensuring adaptability to evolving digital threats.

5.4 Analysis of Key Components and Legal Implications of the Resolution

5.4.1 Ad Hoc Committee

The resolution establishes an Ad Hoc Committee to draft a global cybercrime convention. This committee is mandated to convene at least six times, each session lasting 10 days, beginning in January 2022. Decisions within the committee are expected to be made by consensus or, failing that, by a two-thirds majority.

5.4.2 Cyber Sovereignty and Legal Boundaries

The concept of cyber sovereignty presents a significant legal challenge. Countries such as China and Russia advocate for state control over cyberspace, potentially clashing with international norms of internet freedom and openness. The UN resolution seeks to address these tensions, but the broader debate over the degree of state control in cyberspace governance remains unresolved, necessitating a balance between sovereignty and global cooperation.

5.4.3 Public-Private Cooperation and Liability

Legal frameworks must account for the increasing role of private companies in cybersecurity. The resolution encourages collaboration between states and private entities, such as internet service providers and cybersecurity firms, to counter cyber threats. This approach raises legal questions concerning the responsibility and liability of these companies, especially when they participate in responding to or preventing cyberattacks.

5.5 Jurisdictional Provisions (Article 22)

5.5.1 Territorial Jurisdiction

State Parties must establish jurisdiction over offenses committed within their territory or on vessels or aircraft registered under their laws.

5.5.2 Extended Jurisdiction

States may also establish jurisdiction over offenses that:

- Are committed against their nationals.
- Are committed by their nationals or stateless persons habitually residing within their territory.
- Are committed outside their territory with the intent of carrying out an offense within their territory, as specified in Article 17 of the Convention.
- Are committed against the State itself.

5.5.3 Jurisdiction and Non-Extradition

If the alleged offender is present within a State's territory and not extradited solely due to nationality, the State must establish jurisdiction over the offense. In cases where extradition is denied for other reasons, States may take additional measures to establish jurisdiction.

5.5.4 Coordination Among States

When a State exercising jurisdiction becomes aware of other States conducting investigations or proceedings for the same offense, authorities are encouraged to consult and coordinate their actions.

5.5.5 Compatibility with International Law

This Article affirms that the Convention does not prevent any State Party from exercising other forms of criminal jurisdiction, as permitted by its domestic law.

5.6 Garlasco Case

Digital evidence could be altered and can contain countless pieces of information. The "Garlasco" case is a clear example of this.

Alberto Stasi was acquitted of the murder of his girlfriend, Chiara Poggi, by the Court of First Instance in December 2009, and the judgment was confirmed in the Appeal court in December 2011.

5.7 Italian Case Law on Digital Forensics

- **13/08/07:** Stasi wakes up at 9, telephones Chiara Poggi, works on his thesis.
- **14/08/07:** Chiara Poggi died between 10:30 and 12:00.
- **29/08/07:** Stasi voluntarily hands over his PC to the Police.
- **17/12/09:** Judge Vitelli acquits Stasi of murder.

The expert report requested by the judge shows that Stasi was working on his thesis during the period when Chiara Poggi was killed.

5.8 The Internet of the Human Body: Towards a Habeas Data?

> "If your internet thermostat's pinging servers all day, will the cops think you're a weed farm? Or just a hot yoga gym?"
> *Jonathan Zittrain*

> "Sure, encrypt your email – while your shiny IoT toothbrush spies on you"
> *Susan Landau*

5.9 Cases

5.9.1 Connie Debate Case: Fitbit

> "As people continue to provide more and more personal information through technology, they have to understand we are obligated to find the best evidence, and this technology has become a part of that."
> *Detective Christopher Jones - East Lampeter Township Police Department in Pennsylvania*

> "We are entering an era of sensorveillance. People are just waking up to the fact that their smart devices are going to snitch on them and that they are going to reveal intimate details about their lives they did not intend law enforcement to have"
> *Andrew Ferguson, a University of the District of Columbia law professor*

5.9.2 James Bate Case: Amazon Echo

> "The Amazon Echo device is constantly listening for the 'wake' command of 'Alexa' or 'Amazon,' and records any command, inquiry, or verbal gesture given after that point"
> *Search Warrant*

> "The allegation that the Echo is possibly recording at all times without the wake word being issued is incorrect"
> *Answer of an Amazon Representative*

There are prloblems with the term and conditions of the Amazon Echo, as they are record data even without the wake word being issued. This is also correlated with all the problem reguardind the user of dark pattern for avoid that the use could block this kind of data collection.
In another case Amazon refused to give data collected by an Amazon echo to the police and use the term and conditions as exuse.

NOTE: particularly attection for device that arrive from China (alsways check the user term and conditions).

5.9.3 Ross Compton Case: Pacemaker

> "There is a lot of other information about things that may characterize the inside of my body that I would much prefer to keep private rather than how my heart is beating. It is just not that big of a deal"
> *Judge Charles Pater*

> "Americans shouldn't have to make a choice between health and privacy. Compelling citizens to turn over protected health data to law enforcement erodes those rights."
> *Electronic Frontier Foundation Attorney Stephanie Lacambra*

Accused of frode from the incusance (hose burn), at the end of the process, the judge accept to aquire the data from the peace maker, to check the beat of the heart at the time of the incident.

Inside our body there are a lot of data that could be used for the investigation, but the question is: how much of this data could be used for the investigation?

5.10 Facial Recognition Biometric Border

> "U.S. Customs and Border Protection says it will delete the live photos captured at the gate within 14 days for citizens, and that it only uses them to verify identity by comparing them with the database photos"
> *CBP Privacy Impact Assessment*

> "Face Recognition has a great potential for expansion and misuse: for example, you can subject thousands of people to face recognition when they're walking down the sidewalk without their knowledge"
> *Senior Policy Analyst, ACLU - Jay Stanley*

In europe there is a law that proibit the use of facial recognition in real time for the identification of the people, but in the US this is not the case.

5.11 Categories of Law Enforcement Activity

- Situations involving officers observing an ongoing crime (**FaceFirst**)
- Situations involving officers investigating a past crime **(KeyCrime[3])**
- Situations involving officers predicting a future crime (**PredPol**, used in US, illegal in EU for AI act)
  Tool for analysze crime that could happen in the future baed on the use of bigdata from the db of the law enforcement and social media data.
  The problem for the critisim is that if you predict a crime in a certain area, the police will go in that area and this could lead to a self-fulfilling prophecy.

5.12 "Police" Directive

The Pocile Directive can be seen as a GDPR for the police. It is composed by 5 pillars:

- Fairly, lawful, and adequate data processing during criminal investigations or to prevent a crime
- Clear distinction of various categories of data subjects in a criminal proceeding (investigated person, person convicted, victim of crime, third parties to the criminal offense)
- Prohibit measures that produce adverse legal effects for the data subject based solely on automated processing of personal data
- Implementation of privacy by design and by default mechanisms to ensure protection of data subject rights and minimal processing
- Cooperation with relevant supervisory authorities, providing all necessary information for their duties

5.13 Automated Processing (Article 11 - "Police Directive")

Automated processing is forbidden unless:

- **Human Intervention:** Automated processing is forbidden unless:
  i. There is human intervention
  ii. Produce an adverse legal effect concerning the data subject
  iii. Is authorized by UE or Member states
  iv. Provides appropriate safeguards for the rights and freedoms of the data subject

- **Profiling:** Profiling that results in discrimination against natural persons on the basis of special categories of personal data referred to in Article 10 shall be prohibited, in accordance with Union law.
- **Access to electronic:** Legislation permitting public authorities to gain access to the contents of electronic communications on a generalised basis must be regarded as compromising the essence of the fundamental right to respect for one's private life, as guaranteed by Article 7 of the Charter

5.14 Transparency, Retention, and Enforcement

- **Transparency**: Tools based on big data for law enforcement purposes is checked by the law enforcement authority prior to final purchase and can be verified for its suitability, correctness and security, bearing in mind that transparency and accountability are limited by proprietary software
- **Retention**: While EU legal framework on data retention still lacking and we are waiting the Guidelines, safeguards are required for data retention to be lawful according to the ECJ case law are:
    i. serious crime;
    ii. necessary and proportionate retention measure;
    iii. national authorities' access should meet certain data protection safeguards
- **Enforcement**: Member States shall lay down the rules on penalties applicable to infringements of the provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive

5.15 Privacy vs Security

What happens if security prevails over privacy? - Netflix case

5.16 Budapest Convention on Cybercrime - Overview

The Budapest Convention on Cybercrime was issued by the Council of Europe on November 23, 2001. Italy ratified the Convention with Law n. 48 on March 18, 2008, and it was published in the Official Gazette on April 4, 2008.

Chapter 6

Hacking Team Case Study

6.1 Hacking Team Case

6.2 Background on Hacking Team

Hacking Team was an Italian technology company primarily known for its offensive intrusion and surveillance software provided to government bodies and law enforcement agencies across the globe. Established in 2003, the company garnered significant controversy due to its practices and clientele, which included both national security organizations and regimes with questionable human rights records.

6.2.1 Company Overview

- **Founded:** The company was established in Milan, Italy, by David Vincenzetti in 2003.
- **Business Model:** Hacking Team specialized in creating and selling offensive cybersecurity tools tailored for governmental and law enforcement agencies, focusing on hacking and surveillance applications.
- **Key Clients:** The client list reportedly included major international organizations such as the NSA, CIA, FBI, and other international law enforcement agencies.

6.3 Core Technologies

Hacking Team developed advanced tools to enhance surveillance capabilities for their clients, often pushing the boundaries of intrusion technology.

6.3.1 Remote Control System

A software solution enabling monitoring of Internet communications, data decryption, and activity tracking.

6.3.2 Mobile Surveillance

Technologies designed for tracking cell phones, monitoring calls, and intercepting messages.

6.3.3 Remote Activation

Tools capable of remotely activating microphones and cameras on target devices, including precise location tracking.

6.3.4 Advanced Surveillance Techniques

- **Battery Optimization:** Techniques to minimize battery usage on monitored devices, reducing suspicion from the target.
- **Stealth Operations:** Surveillance procedures developed to be highly undetectable.
- **Data Extraction:** Sophisticated methods to extract and analyze data from target devices effectively.

6.4 Founding and Early Years

- **2003:** David Vincenzetti and Valeriano Bedeschi founded the company in Milan.
- **2007:** Hacking Team received $8 million in funding from Italian venture capital, supporting rapid growth.
- **Early Success:** The Milan police purchased Hacking Team's software, marking it as one of the first providers of commercial hacking solutions.

6.5 Applications of Technology

Hacking Team's technology was applied in various high-stakes operations by law enforcement agencies around the world.

- **Counter-Terrorism:** Utilized to monitor and track terrorist activities, assisting in prevention and response.
- **Drug Trafficking:** Employed in combating international narcotics trade by tracking and intercepting key individuals and communications.
- **Organized Crime:** Used to gather intelligence on mafia and other criminal organizations.

6.6 High-Level Connections

- **Booz Allen Hamilton:** Established connections with Mike McConnell, a former NSA director and influential intelligence advisor.
- **US Intelligence:** Collaborated with the NSA, CIA, and FBI, highlighting its close ties with American intelligence.
- **Global Reach:** Extended operations to intelligence agencies worldwide, solidifying its position in international cybersecurity markets.

6.7 Saudi Arabia Acquisition Attempt

- **2013:** Initiated acquisition discussions with the Saudi Arabian government.
- **Valuation:** The company was valued at $2 billion, though Saudi Arabia's offer was approximately $140 million.
- **Mediators:** Wafic Said, Britain's third wealthiest Arab billionaire, was involved as a mediator in negotiations.

6.8 Controversial Clients

Hacking Team faced criticism for dealing with governments known for human rights abuses.

- **Sudan:** Software was sold to Sudan, despite an arms embargo imposed by the United Nations.
- **Bahrain:** Provided surveillance technology to the Bahraini government.
- **Saudi Arabia:** Supplied spyware to Saudi Arabian authorities, sparking international concerns.

6.9 UN Investigation

- **June 2014:** The United Nations commission raised concerns about Hacking Team's sales to Sudan.
- **January 2015:** Hacking Team denied any ongoing sales to Sudan.
- **March 2015:** The UN suggested that Hacking Team's software could be classified as military-grade equipment.

6.10 Italian Export Ban

- **Autumn 2014:** The Italian government temporarily suspended Hacking Team's export license.
- **Lobbying Efforts:** Hacking Team engaged in lobbying to reverse the export restrictions.
- **Ban Lifted:** The company ultimately regained the right to sell its products internationally.

6.11 Ethical Concerns

Critics raised ethical issues regarding Hacking Team's operations and clientele.

- **Human Rights:** Accused of enabling surveillance in regions with poor human rights protections.
- **Privacy Violations:** Tools were often used to infringe on citizens' privacy rights.
- **Democratic Concerns:** Allegations of contributing to the suppression of democratic freedoms in certain nations.

6.12 Legal Challenges

- **UN Sanctions:** Faced scrutiny regarding potential violations of the UN arms embargo.
- **Italian Export Laws:** Temporary suspension of exports by the Italian government.
- **Privacy Lawsuits:** Involved in legal actions in various countries related to privacy violations.

6.13 The Investigation

6.14 2015 Data Breach

In 2015, Hacking Team, ironically known for its surveillance and cybersecurity tools, became a victim of a significant cyber attack. This event had far-reaching consequences for the company and its clients.

6.14.1 Event

Hacking Team's internal systems were breached, leading to the unauthorized access and exposure of confidential information.

6.14.2 Consequence

Approximately 400 gigabytes of sensitive data were leaked, including emails, financial documents, and client communications.

6.14.3 Aftermath

The breach publicly revealed the company's internal operations, client lists, and previously confidential dealings, casting a negative spotlight on Hacking Team's business practices and clientele.

6.15 Client List and Revenue

Hacking Team's client base and revenue streams were broad, involving high-profile organizations and substantial financial engagements.

6.15.1 Client Types

Primarily served military, police, governmental, and intelligence agencies worldwide, providing them with hacking and surveillance tools.

6.15.2 Corporate Clients

The company maintained partnerships with multinational corporations, including Boeing, expanding its influence beyond public sector organizations.

6.15.3 Revenue

Hacking Team reported annual revenues exceeding €40 million, though some reports suggested additional income from larger, undisclosed offshore contracts.

6.16 Milan Prosecutor's Investigation

Suspicious financial transactions led to an official investigation by Milan's prosecutor's office, which scrutinized dealings between Hacking Team affiliates and external entities.

6.16.1 Trigger

A suspicious payment from a Saudi Arabian company to SoftHack Srl, a Turin-based firm, prompted Milan prosecutor Alessandro Gobbis to order a search of SoftHack Srl.

6.16.2 Action

The prosecutor launched an investigation, focusing on possible unauthorized sales or misuse of Hacking Team's spyware technology.

6.16.3 Suspicion

It was suspected that the Galileo spyware source code may have been illicitly sold to unauthorized parties, raising concerns about its potential misuse.

6.17 SoftHack Srl Investigation

SoftHack Srl, the company at the center of the suspicious transaction, became the subject of legal scrutiny.

6.17.1 Company Details

SoftHack Srl, based in Turin, is a technology company involved in software development.

6.17.2 Individual Involved

Luca Spector, a developer associated with SoftHack Srl, was investigated under charges of unauthorized system access and disclosure of industrial secrets.

6.18 Suspicious Transaction Details

Details of the payment that triggered the investigation are as follows:

- **Date:** November 20, 2014
- **Amount:** 300,000 euros
- **Sender:** Saudi Technology Development Inv.
- **Recipient:** SoftHack Srl

6.19 Prosecutor's Suspicions

The Milan prosecutor's office raised concerns regarding the nature and intent of the transaction.

6.19.1 Cover Story

The payment was reportedly for "professional training services"; however, this explanation was met with skepticism.

6.19.2 Real Purpose

Investigators suspected that the true intent of the transaction was the sale of the Galileo spyware source code.

6.19.3 Potential Misuse

There were concerns that the software could potentially fall into the hands of terrorist groups or be misused for malicious purposes.

6.20 Saudi Technology Development Inv

The investigation further examined Saudi Technology Development Inv., the company involved in the suspicious payment.

6.20.1 Investigation Focus

The probe focused on the shareholders of the company and any potential connections to jihadist networks.

6.20.2 Intermediary Role

Saudi Technology Development Inv. was suspected of acting as a mediator for an unidentified client, raising questions about the true end-users of the spyware.

6.20.3 Unknown Motives

The motivations behind the acquisition of Hacking Team's software by this entity remain unclear.

6.21 SoftHack's Defense

SoftHack Srl and its legal representation denied any wrongdoing and provided clarifications regarding the transaction.

6.21.1 Denial

SoftHack's lawyer refuted the accusations, claiming they were baseless rumors propagated by Hacking Team.

6.21.2 Clarification

The defense pointed out that the search warrant did not explicitly mention any sale of services to Arab or terrorist organizations.

6.21.3 Transparency

SoftHack expressed a willingness to cooperate fully with the investigation to demonstrate its innocence.

6.22 Ongoing Investigation

The investigation continues as authorities delve deeper into the background and potential connections of Saudi Technology Development Inv.

6.22.1 Current Focus

Efforts are centered around investigating Saudi Technology Development Inv.'s history and any links it might have to extremist groups.

6.22.2 Key Question

A primary focus of the inquiry is determining whether the spyware ultimately reached terrorist organizations or other unauthorized users.

6.22.3 Next Steps

The investigation will proceed with additional interrogations and analysis of financial transactions to ascertain the true nature of the dealings.

6.23 Search and Seizure

6.24 Subject: Search and Seizure of Electronic Devices

6.24.1 Issuing Authority

The Italian Cybercrime Unit issued a search and seizure warrant directed at SoftHack Srl's headquarters in Turin. This warrant was part of a broader investigation initiated by the Prosecutor's Office of Milan.

6.24.2 Location to be Searched

The search specifically targets the main offices of SoftHack Srl in Turin.

6.24.3 Items to be Seized

The warrant details several categories of electronic devices that are believed to contain critical evidence for the ongoing investigation:

- Laptop computers
- Smartphones
- CCTV cameras
- Tablets (including iPads)
- Other electronic devices capable of storing digital evidence relevant to the case

6.24.4 Purpose of Warrant

The warrant is part of an investigation into unauthorized access to proprietary source code owned by Hacking Team, a Milan-based intelligence software company. Evidence suggested that SoftHack Srl may have received substantial payments from Saudi Technology Development Inv., which were allegedly labeled as payments for professional training but are suspected to be in exchange for sensitive source code and proprietary information.

6.25 Justification for Immediate Seizure

The presence of specified electronic devices at SoftHack Srl is believed to hold critical evidence essential to the investigation. Immediate seizure was authorized to prevent any tampering, destruction, or concealment of data. Preserving digital evidence in its original state is necessary to maintain evidential integrity in accordance with digital forensic protocols.

6.26 Digital Forensics Standards

The execution of the warrant adheres to strict digital forensic principles to ensure evidence integrity and admissibility in court:

6.26.1 Integrity of Evidence

All electronic devices must be handled carefully to prevent any data alteration. Forensic experts are tasked with securing the devices in a controlled environment, using write-blocking tools and creating forensic images of all data prior to any detailed examination.

6.26.2 Documentation and Chain of Custody

A comprehensive log of each device seized must be maintained, detailing serial numbers, device types, and any identifiable markings. The chain of custody is recorded from the moment of seizure to the forensic examination, ensuring full transparency and traceability.

6.26.3 Impartiality and Accuracy

Digital forensics standards are strictly enforced to prevent contamination or bias. Write-protection technology and forensic imaging are essential to preserving original evidence without alteration.

6.27 Execution of the Warrant

The warrant authorizes the Italian Cybercrime Unit to enter and search the premises of SoftHack Srl, with specific attention to the electronic devices listed above. The search is to be conducted within a specified timeframe, after which all seized devices will be transferred securely to a designated forensic lab or another appropriate authority for analysis.

6.28 Additional Provisions

- The warrant restricts access solely to data relevant to the investigation, and private data unrelated to the case must remain protected.

- All procedures are to comply with applicable data protection laws, thereby respecting the privacy of individuals not associated with the investigation.

6.29 Order

The Prosecutor's Office of Milan issues this search and seizure warrant to be executed in accordance with the outlined digital forensic standards. The order emphasizes the importance of maintaining forensic reliability and preserving all digital evidence collected during the search.

6.30 Guidelines for Prosecutor and Law Enforcement Officers

To ensure compliance with digital forensic principles throughout the investigation, prosecutors and law enforcement officials should adhere to the following:

- Respect the chain of custody and document all procedures accurately.
- Utilize forensic imaging and write-blocking tools to safeguard the original state of electronic evidence.
- Ensure the impartial handling of evidence to avoid introducing bias.

6.31 Defense Strategy and Attorney's Role

6.31.1 Attorney's Responsibilities

The defense attorney has a critical role in protecting the defendant's rights during the investigation:

- Ensure that forensic protocols are followed, and that evidence was collected and handled legally.
- Advocate for the preservation of the defendant's rights, particularly regarding privacy and protection from unlawful search and seizure.

6.31.2 Demonstrating Client Innocence

To demonstrate the innocence of the defendant, the attorney should:

- Scrutinize the validity of the evidence, ensuring it was obtained without bias or procedural errors.
- Gather any exculpatory evidence or alternative explanations that might counter the prosecution's allegations.
- Present compelling evidence to the judge, providing context to support the client's lack of involvement in the alleged wrongdoing.

Part II

Tech

Chapter 7

Introduction

7.1 Topics

- **Forensics Analysis**
  use of logic and meaningful knowledge and methodological approach to legal problems and criminal investigation.

- **Computer Forensics**
  Collection, preservation and analysis of digital evidence (inside file system, email, cloud account etc...) to support investigation and legal proceedings

7.2 Forensics History

7.2.1 Ancient Times

Forensic science dates back to **Babylon (1900 BC)** where fingerprints were used for identification, and **China (1248 AC)** with forensic pathology. In the **UK (1835)**, bullet comparison solved a case, and by **1892**, the first murder was solved using fingerprints.

7.2.2 Modern Times

Forensic standards grew in police departments, with the first crime lab in **1923**. DNA fingerprinting began in the **1950s**, and DNA profiling was developed by **1985**. **AFIS** systems emerged in the late **1980s**. Today, AI, toxicology, and digital forensics are key areas of innovation.

7.2.3 Digital Field

Early Times

In **1989**, Robert Morris was convicted under the Computer Fraud and Abuse Act, marking the first use of computer logs in forensics. That year, **IACIS** was founded, followed by **IOCE** in **1995** to share digital forensic practices.

Recent Times

- **1990**: Forensic tools like EnCase emerged

- **2000**: Digital forensics became widespread in law enforcement

- **2010**: Growth of cloud and mobile forensics, automation, and machine learning
- **2020**: Advances in crypto, blockchain, and AI improve digital forensics

7.3 Computer Forensics Definitions

US_CERT: The discipline that combines elements of law and computer science to collect and analyze data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law.
A. Ghirardini -Computer Forensics: The discipline whose goal is preservation, identification, analysis of information system to the aim of identification of evidences during investigation activities.
NIST glossary: The application of computer science and investigative procedures involving the examination of digital evidence - following proper search authority, chain of custody, validation with mathematics, use of validated tools, repeatability, reporting, and possibly expert testimony.

7.4 CF purpose(s)

7.4.1 CF Q&A

During an investigation, digital forensics need to analysis data to answer some key questions:

- **What happened?**
- **Who was involved?**
- **When did it take place?**
- **Where did it take place?**
- **Why did it take place?**
- **How did an incident occur?**

The answers to these questions are essential for support legal proceedings and mitigate possibility of future incidents with a preventive approach.

7.4.2 CF Goals

The goals of computer forensics (CF) are multifaceted and aim to provide a comprehensive understanding of digital incidents.
Firstly, CF seeks to retrieve what has been the input, such as what has been typed. It also aims to determine the actions performed, for example, what programs have been run and what peripherals have been connected. Additionally, CF involves analyzing used files to understand what modifications have been done and when these modifications occurred (and the information from an OS are not enougth, because are an abstraction managed by the file system → needed bit analysis (like for ereased data)).
Another critical goal is to identify the damage done, such as what data have been erased. In essence, the overarching goal of CF is to **gain a technical comprehension of what happened during the incident** (from a technical point of view).

Chapter 8

CF Terminology & revelant conceps

8.1 Terms

8.1.1 Digital evidence

Technical definition of Digital evidence is very similar to the legal ones:

> Data stored or transmitted in digital form that can be used in court.

The conrnerstones of digital forensics are the different levels of **abstraction**, requires **interpretation**, are **fragile**, may be **voluminous** and the difficulty to discover **connection** between data and reality (the connection need to be done beafore entering the court).

Digital evidence also requires a deep technical understanding of the possible types of data (files, emails, logs, metadata) and the legal requiremnets for each of one to collect and preserve it. (To make all of this effective, knowledge of file systems, network protocols and encryption are essential)

8.1.2 Chain of custody

> Documented and **unbroken** process of handling evidence from the time it is collected until it is presented in court

This procedure is essential to ensure the integrity of the evidence and to avoid that them to be tampered or accessed by unauthorized people.
Keep the chain of custody requires knowledge about how to document evidence collection, storage, and access (logging procedures, secure storage, legal prtocols etc..)

If the chain of custody is **broken**, the evidence may be considered **inadmissible in court** (so is needed know the regulation of the state to decide how to manage it).

8.1.3 Data acuisition

> The process of collecting digital evidence from devices without altering or damaging the original data.

One of the biggest problem fo the managment of digital evidence, because it's needed to be performed on hostile systems (that can be infected, compromised, have a malware or system to avoid copy like edited system call for make other program to fail). in a not coltrolled envorment like a crime scene.
So are needed knowledge of disk imaging and live data capture in order to not alter what's going on on the suspect system. Are also required expertise in forensics acquisition, analysis tools (like FTK Imager, EnCase) and knowledge of file systems, write-blockers, and hashing (crucial for ensuring integrity).

8.1.4 Hashing

> The process of converting data into a fixed-length string of bits, which represents the data uniquely

It's used in the chain of custody for ensure the integrity of the digital evidence and so verity that a file has not been altered.
Require understanding of hashing algorithms (strengths and weaknesses, e.g. MD5 collision), formats (hex, base64 etc...) (if wrong formats are sued, the chain of custody is broken and each information gathered from that point is considered not valid) and expertise in hashing tools (sha256sum, hashdeep, FTK imager, Autopsy).

Have to be used any time an evidence is "managed" (copied, moved)

8.1.5 Write Blocker

> Hardware or software tool used to prevent any data from being written to a storage device during analysis, preserving the original data content

To be operated, require understanding of how write-blocking devices work and how they can be implemented in forensic procedures.

It's essential for the legally defensible acquisition.

8.1.6 Forensic image

> A bit-by-bit copy of digital media, including deleted files and data in slack space, which is an exact replica of the original device

The goal of a forensic image is to preserve the original evidence and aovid the modification of the original data.

To be performed in a correct way, requires understanding of mechanisms to copy information in digital devices (file system knowledge and behavior) and familiarity with with bit-by-bit copy tools (DD, FTK Imager, EnCase, Guymager).

As the hashing, it's need to be used any time an evicene is "managed" (copied, moved)

8.2 Scenarios

There are some possible scenario that a computer forensic investigator can face:

- Internet abuse from employee
- computer-aided frauds
- Data unauthorized manupulation (theft or destruction)
- Computer/network manage assessment
- ... any other case that include digital evidence

8.3 investigation phases

A Computer forensics investigatos usually follow standard phases that guide him. There are different standards like: NIST family, ACPO guidelines (UK), ISO/IEC 27042, SWDGE.

8.3.1 Phases

- **identification:** When the investigator come for the first time to the crime scene and need to identify potential source of relevant digital evicences.
- **collection:** The letteral pick up of the evidence (like a computer or a smartphone) or a remote taking possession of the evidence (like for a remote server) and its connection (e.g. network or physical, like USB disk).
  It's splitted from acquisition because it's a critical phase where the evidence can be altered and lost utility for the investigation (es. data corruption, lost of metadata etc...)
- **acquisition:** Electronically retrieving data by running various CF tools and software suites
- **evaluation:** Evaluating the data recovered to determine if and how it could be used against the suspect (e.g. for prosecution in court)
- **presentation:** Presenting the evidence discovered in a manner which is suitable for lawyers, non-technical staff/management and the law (and internal rules)

8.3.2 Identification

During the identification phase is important **recognize** all the **relevant data sources** before any acquisition, even if no physical present, like data in the cloud
A imple **list of example** are: hard drives (HDD/SSD), memory (RAM), mobile devices (smartphones, tablets), cloud storage, network traffic, removable media (USB drives, DVDs), IoT devices and embedded systems (like smart washing machines)
For identify these sourcer, the investigator can perform some actions, like:

- Perform an initial survey of the scene (physical or network environment)
- Identify key devices and data locations (local storage, remote servers, cloud services)
- Check for connected devices, including peripherals like printers, removable media, or network-attached devices
- Map all potential data sources using network topology diagrams or asset inventories

A particolar aspect that need to be considered is the possible present of "ephemeral" storage or data, like cloud syncing, hidden secttor, tmp, dat in ram etc...

8.3.3 Collection

During the collection, the focus is on gathering evidence from identified data sources while ensuring the preservation of its integrity. An important key point is the implementation of methods that **minimize the risk of evidence tampering or data loss**.
For enforce this key point, it's importnat **isolate devices** to prevent them from being tampered with remotely (e.g., disconnect them from the network), use devices to **block external communication** for mobile or wireless devices and use network isolation tools for virtual and cloud environments to prevent remote access (like use a virtual private cloud).
A particular note is for the managment of live systems where is needed ensure evidence integrity while maintaining system uptime (so not shoutting down the system for avoid the loss of volatile data).
Create a **detailed record** of the condition and state of the evidence

- take photographs of the devices in situ, including connected peripherals and the physical state
- record serial numbers, device models, and any other identifiable information
- document the scene, noting which devices were running, whether screens were active o locked, and any other visible indicators

hint: complete documentation is crucial to prevent legal challenges regarding the integrity of the evidence.
Beafore procede to the acquisition, is needed to ensuring no alteration will take place, so do somethings like enable write blockers for physical storage devices, disalbe connection and sinking. particulary complex is maintain integrity on live systems (e.g., using remote collection methods that minimize data alteration risks)

8.3.4 Acquisition

The act of performing a forensic copy (so a bit-by-bit copy) of the original data with the goal of ensure that the acquired data is a faithful replica of the source so to maintaining data integrity.
There 2 two main acquisition methods:

- **Static:** When the system is powered down, it's se most commod method for acquiring data from hard drives and extenral memory
- **Live:** The system is running and it's needed to deal with volatile data like RAM, network connections, or running processes.

Static acquisition

1. shut them down carefully to avoid losing data
   • e.g. for encrypted devices, consider methods for capturing data without triggering loss of access (e.g., before the decryption key is wiped from RAM)
2. attach the device to a forensic workstation using a write blocker
3. use forensic imaging tools to create a complete image of the storage device
4. generate a hash value (e.g., SHA-256) of the original media before and after acquisition to verify integrity
5. store the image on a secure forensic storage device

hint: pay attention that data is properly hashed and verified post-acquisition, not perform steps like an automata.

Live acquisition

1. choose a method that minimizes system interference while capturing volatile data
2. dump RAM (memory acquisition) and capture data from running processes or network connections.
3. perform network traffic capture
4. document all acquisition actions and steps to ensure chain of custody and admissibility
5. hash the volatile data wherever possible to maintain data integrity

Integrity

In this phase is needed to ensure that the acquired data is an exact replica of the original and has not been altered.
Performed mainly by the use of hashing algorithms.
Some general steps are:

- choose a method that minimizes system interference while generating a hash (MD5, SHA-256) of the acquired image or data dump
- compare the hash value to the original data hash (for static data) to verify its integrity
- document the hashing process, including the algorithms used and the results, in the chain of custody documentation

hint: be careful! any discrepancies in hash values would require re-acquisition and could damage the credibility of the evidence

Chain of custody

This section need to be performed in paralled with all the other phases to ensure a complete, documented chain of custody for the evidence throughout the acquisition process. (Record every step in the acquisition process, including personnel involved, tools used, date, and time of acquisition.
Store the data and evidence securely to avoid unauthorized access or tampering)

8.3.5 Evaluation

analyzing, verifying, and validating the evidence to ensure it remains unaltered and trustworthy for legal proceedings or further analysis. It's possible alter the evidence only if the evaluation is performed on a copy of the original data.
More in practice, the main actions that are performed are:

- timestamp and metadata analysis
  - verify file creation, access, and modification dates of data to ensure they match the timeline of the incident
- timeline reconstruction
- cross-reference analysis/consistency verification
  - correlation of digital evidences with external logs or other data to countercheck it is related to the suspected system or device

  - comparison of data from different sources (e.g. logs, email)

- compliancy with current legal/internal standards

  - collection, preservation, evaluation must be coherent to applicable legal procedures...and the documentation must keep track of that

- review of possible anti-forensics techniques

8.3.6 Presentation

Preparing and presenting the findings of the investigation in a clear, accurate, and legally admissible manner is essential. The goal is to **translate** the technical details of the forensic analysis into a format that can be understood by **non-technical stakeholders**, such as lawyers, judges, or company executives.

Hint: The quality and clarity of the presentation can significantly influence the outcome of legal proceedings or internal investigations.

Actions:

- Review all the data collected, analyzed, and interpreted during the investigation.
- Identify the key pieces of evidence.
- Verify that all conclusions are directly correlated to verifiable evidence.
- Document the entire forensic process in a formal report, free from technical jargon, so that it can be submitted as legal evidence.
- Securely manage the report to ensure its integrity.

Hints:

- Avoid "personal interpretation" unless explicitly asked to provide expert opinion.
- Include appendices with timestamps, metadata, hash values, and other forms of technical evidence as "reinforcement."

Chapter 9

Non-trusted environment issues

We need to not trust an enviroment by default, becasue it can be compronised, and there are many ways to do so.

9.1 Compromise causes

9.1.1 Node infection

Nowadays, a node infection is obtained through a social engineering attack, that lead to the download of a compromise file/software.

- Legitimate software containing malicious code (trojan horses) (a free version of paied software is alsways a good bait), social engineering, physical access, bug or configuration error exploitation (OS syscall, device driver, application, firmware and BIOS, browser ...)
- Backdoors creation, data stealing, hidden (or not so much) processes disruption, ...
- Persistent unauthorized access to a system (as root - i.e. rootkits)
- Spyware (sensitive information collection)
- Ransomware (encryption of sensitive data)

9.1.2 network injection

- nodes capable to read and write data while in transit, actors capable to ”poison” routing mechanisms
- access and modification of network data flow, redirection versus illegitimate destination
- Sniffers and (growing) family of Man-in the-X attacks

9.1.3 supply chain attacks

- compromise of service, hardware, software of a third-party vendor or partner used (and trusted) by the target organization
- gain access to the target organization, inject unauthorized behavior
- infrastructure for update management
-
    - e.g. SolarWind Orion Attack
    - malicious code into software updates of Orion network monitoring platform.
    - distributed to over 18,000 customers, including government agencies and large corporations.

- libraries and dependencies
- hardware during manufacturing
- IT infrastructure management service
- ...

9.1.4 Men at work

man-in-the-middle

An attacker secretly intercepts or alters communication between two unaware parties.
Examples include **HTTP session hijacking**, where the attacker intercepts session cookies to impersonate a user, and **ARP table poisoning**, where ARP tables are altered for traffic redirection.

man-in-the-browser

Infection occurs in the browser to alter web pages or transactions.
An example is banking trojans like **ZEUS**, which modify online transactions.

man-in-the-cloud

This involves stealing credentials or tokens to access a user's cloud environment.
For example, the interception of a Google Drive OAuth token can allow access to the victim's files.

man-in-the-mobile (MitMo)

Mobile infection is used to intercept communication or two-factor authentication (2FA).
An example is ZitMo, which intercepts SMS and forwards them to a command and control (C&C) server.

man-in-the-disk

This exploits vulnerabilities in handling external storage.
For instance, an attacker can modify temporary files stored on an external device.

man-in-the-memory (MitMem - guest star)

In this case, an attacker intercepts or modifies data while it is in RAM.
A notable example is fileless (stealth) malware.

man-on-the-side

An attacker observes and injects communication without modifying it.
An example is China's Great Cannon.

man-at-the-end

This type of attack compromises end-point communication.
For example, a keylogger infection can capture sensitive information.

9.2 Advanced persistent threats (APT)

- **advanced**
  - use of sophisticated techniques
    - customised malware, zero day vulnerabilities, evasion stategies
  - targeted to specific victim
    - high budget and expertise, careful preparation
- **persistent**
  - Item compromise maintained for extended period
    - possible escalation and infection diffusion
  - low-profile operation (during infection)
    - stealth techniques, limited bandwidth usage, mimicking legitimate traffic
- **threat**
  - highly skilled individual aiming strategic goals (espionage, foreign country intelligence, ...)

9.2.1 APT Attack Process

The Advanced Persistent Threat (APT) attack process consists of several key stages:

Initial Intrusion

The attacker gains access through a weak entry point, such as exploiting zero-day vulnerabilities or using spear phishing techniques to infiltrate the target system.

Foothold Establishment

Once access is gained, the attacker sets up persistent access by installing backdoors or infecting the system with (stealth) malware to maintain control over the compromised environment.

Privilege Escalation

The attacker escalates privileges to gain further control over the target system. This involves techniques like credential stealing or vulnerability exploitation.

Lateral Movement

The infection spreads across the target organization as the attacker moves laterally (like over different device/account with same/similar level of privilage), using stolen credentials (social eng.) or exploiting vulnerabilities to compromise additional systems.

Goal Achievement

The attacker eventually reaches their goal, which often involves data exfiltration or sabotaging critical systems.

9.2.2 manupulation from the system owner

If the system ownert is technical-savy, he can manipulate the system to hide the compromise, or to make it more difficult to detect, by installing modified application, compromised drivers or edit system calls.

9.2.3 APTxx

APTxx refers to organized hacker groups involved in advanced persistent threat (APT) activities. An example of such a group is **APT28**, also known as Fancy Bear.

APT28 (Fancy Bear)

APT28 is a **Russian state-sponsored group** that operates during Russian business hours and closely aligns with Russian government strategic interests, particularly in regions like the Caucasus.
The group has been active since the mid-2000s, with documented operations dating back to at least 2008. APT28 targets a wide range of sectors, including aerospace, defense, energy, government, media, and dissidents, engaging in activities such as espionage, political influence, and cyberwarfare.

Notable Attacks: In 2016, APT28 was responsible for the breach of the **Democratic National Committee** (DNC) during the U.S. presidential election. This attack led to the leakage of sensitive information with the intent of influencing the election outcome.
Another major attack occurred in 2017 with the NotPetya ransomware, which was initially designed to target **Ukrainian institutions**. However, the malware spread globally, causing billions of dollars in damages.

APT28 Typical Behavior

APT28 targets a wide range of devices, including desktops, laptops, and mobile phones. It often employs *(spear-)phishing* messages to direct victims to realistic websites for credential harvesting.

- APT28 registers domains that closely resemble legitimate organizations (e.g., `qov.hu.com` for the Hungarian government `gov.hu`).
- It uses URL-shortening services to obscure the true destination of malicious links.

In addition, APT28 delivers highly-realistic and targeted emails, often containing ”weaponized” attachments such as `.docx` or `.pdf` files.
They are alos used to implant custom malware, such as **X-Agent**, a multi-functional malware implant used for:

- Data exfiltration,
- Keystroke logging
- Multiplatform operations (Windows, Linux, Android, and iOS).

After gaining initial access, APT28 actively seeks to harvest credentials through techniques like keylogging and central memory dumping. To evade detection, APT28 adopts various **evasion techniques**, including:

- Malware code obfuscation,
- Use of compromised certificate signatures,
- *Timestomping* (modifying timestamps), and
- Encrypted communication channels.

APT28 also engages in **lateral movement** within the compromised organization by exploiting harvested credentials. This lateral movement involves:

- Remote Desktop Protocols (RDP),

- Windows Management Instrumentation Command-line (WMIC) and `PsExec` to execute commands on remote Windows machines, and
- `SSH` to connect to remote Linux systems.

At this point, APT28 escalates privileges by exploiting harvested credentials or vulnerabilities in the system.

Finally, engages in **data exfiltration** using custom **Command-and-Control (C2)** communication frameworks, such as **Zebra C2**. The exfiltrated data may be optionally compressed, especially if large, and is transmitted via encrypted channels like `HTTPS`, `FTPS`, or even custom protocols.

Although primarily known for espionage, APT28 has also been involved in **destructive attacks**. These include the use of **wiper actions**, such as:

- **KillDisk**, designed to destroy the master boot record, and
- Disk wiping tools, particularly in the energy sector.

9.3 Trusted Environment

The analysis must be performed in a **trusted environment**, as rootkits can **alter the normal behavior** of the operating system, making traditional tools unreliable.
Rootkits are capable of **modifying file system utilities**, such as: `ls`, `cp`, `mv`, and other basic commands.

Additionally, rootkits can intercept and **modify file system calls**. For example, they may intercept system calls like `open()`, `chdir()`, or `unlink()` to avoid displaying or acting on specific files, making it difficult to detect their presence.

9.3.1 (example of) System Call Interception

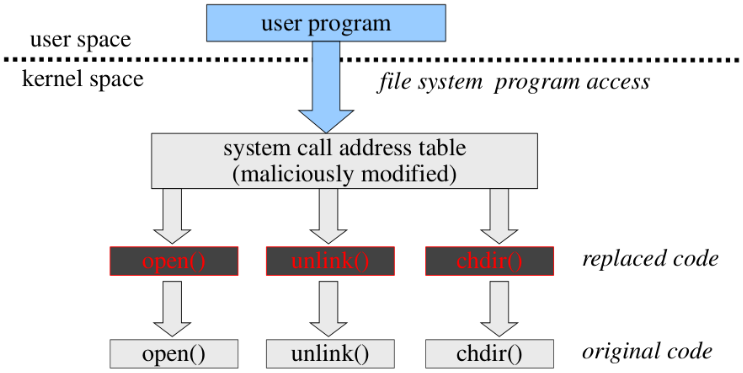


Figure 9.1: Example of System Call Interception

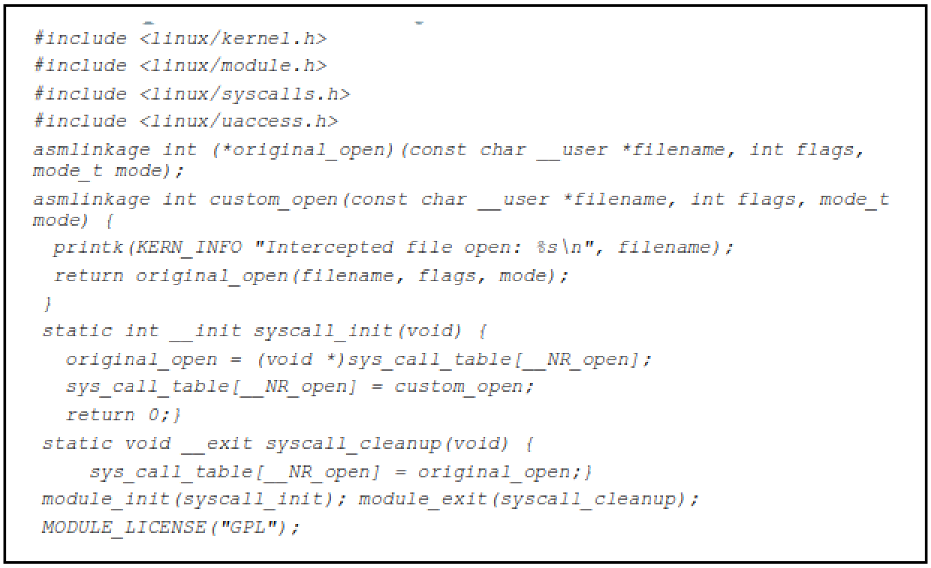
9.3.2 Examples of Linux system modification

A common method of modifying a Linux system is through the use of **Loadable Kernel Modules (LKM)**. This concept is not unique to Linux and can be found in many other operating systems, such as kernel extensions in macOS or kernel-mode drivers in Windows.

An LKM can override the original system call (*syscall*) function. The typical steps to achieve this include:

- **Develop** a modified version of the system call function.
- **Modify** the system call table, which is an array of function pointers, to point to the new version of the function.
- If you want to **modify behavior**, you can re-implement the function with the desired changes.
- If you want to **add functionalities**, enrich the function with additional features and then call the original one to preserve its behavior.

This allows for either enhancing the system with new capabilities or subtly altering existing functionalities without being easily detected.



```
#include <linux/kernel.h>
#include <linux/module.h>
#include <linux/syscalls.h>
#include <linux/uaccess.h>
asmlinkage int (*original_open)(const char __user *filename, int flags,
mode_t mode);
asmlinkage int custom_open(const char __user *filename, int flags, mode_t
mode) {
  printk(KERN_INFO "Intercepted file open: %s\n", filename);
  return original_open(filename, flags, mode);
 }
 static int __init syscall_init(void) {
   original_open = (void *)sys_call_table[__NR_open];
   sys_call_table[__NR_open] = custom_open;
   return 0;}
 static void __exit syscall_cleanup(void) {
     sys_call_table[__NR_open] = original_open;}
 module_init(syscall_init); module_exit(syscall_cleanup);
 MODULE_LICENSE("GPL");
```

Figure 9.2: Examples of Linux system modification

Chapter 10

Tools & Miscellaneous

This section provides an overview of various tools and commands used in Linux for system analysis, troubleshooting, and debugging. Focus is placed on kernel-level information, process control, and signal management, each of which is critical for both routine operations and advanced diagnostics.

10.1 Linux – dmesg

The `dmesg` command is a Linux utility that allows users to:

- Analyze kernel-level details, such as those involved in the system boot process.
- Display messages from the kernel's ring buffer, which includes logs on system boot, hardware detection, driver initialization, and kernel errors.
- View a history of kernel interactions, documenting kernel events like hardware connections, memory allocations, and peripheral issues.
- Engage in system debugging, especially related to hardware, by providing insights into:
  - USB devices, disk errors, CPU issues.
  - Hardware failures or driver errors, which are stored in the kernel logs.
- Access detailed hardware configuration, useful for system configuration and troubleshooting by displaying in-depth information about hardware components.

The `dmesg` command supports various filtering options, enhancing its functionality for more specific diagnostic purposes:

- It can be combined with command-line tools such as `grep` to filter logs. For example, running `dmesg | grep usb` focuses on USB-related logs, which can aid in debugging issues with USB peripherals.
- The command can assist in timeline reconstruction by using the `-T` option, which provides human-readable timestamps for kernel messages. This feature is particularly valuable for tracking the sequence of events in kernel messages.

10.2 Linux – kill

The `kill` command in Linux is both:

1. A function for signal delivery.
2. A shell command that enables users to send signals to processes, instructing them to perform specific actions, such as termination, pausing, or resuming execution.

Key features and functionalities of the `kill` command include:

- Targeting specific processes (or process groups) using the process identifier (PID).
- Offering various signal types, such as:
  - `SIGKILL` for forceful termination.
  - `SIGTERM` for graceful termination.
  - `SIGSTOP` to pause.
  - `SIGCONT` to resume execution.
- Some signals (e.g., `SIGTERM`) can be caught and handled by the process, allowing it to execute cleanup tasks before terminating.
- Permission requirements, where the user needs the necessary privileges to send a signal to a process. Typically, sending signals to processes owned by other users is restricted to enforce security.

The `kill` command is essential for managing and controlling processes within Linux environments, facilitating orderly operations and troubleshooting.

10.2.1 Linux – kill Alteration

In some cases, the use of the `kill` command or mishandling of signals can lead to several issues, including security risks and system instability. Potential alterations and risks include:

- **Incorrect Process Responses:** Signals that are improperly handled can lead to unexpected behavior in processes, such as incomplete shutdowns.
- **Privilege Escalation:** If the `kill` command or underlying processes are modified to bypass permission checks, it can allow unauthorized signal delivery to processes owned by other users. This may enable manipulation of critical services and breach security policies.
- **Persistence:** Ignoring or mishandling signals can result in processes that become ”runaway” or persistent, leading to system degradation. For example, rootkits may be designed to ignore `SIGKILL` signals, making them difficult to terminate.
- **Monitoring Compromise:** Signals often trigger logging or monitoring actions. For instance, some services reload configurations upon receiving `SIGHUP`. If compromised, these monitoring functions may be hindered or disabled.

Chapter 11

Digital Forensics lab set-up

Chapter 12

File system forensics domain // Da completare

The field of file system forensics is focused on analyzing file systems to retrieve hidden or deleted data. This domain is essential for forensic investigations as it uncovers information about the organization and structure of file storage, even after files have been deleted.

12.1 File System Forensics

Key aspects of file system forensics include:

- **Slack Space Analysis:** Investigating unused portions of disk sectors which may still contain residual data from previously stored files.
- **File Carving:** Recovering deleted files by analyzing data remnants in disk clusters, a method useful when files have been deleted but not overwritten.
- **Registry and Configuration Analysis:** Retrieving user or system activities from OS configurations, such as the Windows Registry or Unix configuration files (e.g., `/etc`, `/̃.config`, `/̃.bashrc`). (this part of the analysis is usually done during the OS forensics)

Common tools in this field include low-level utilities like `stat`, `istat`, and `debugfs` as well as high-level software such as FTK Imager and Autopsy.

12.2 File System

A file is the smallest logical unit of storage from the user's perspective, organized into bytes, lines, or records. File systems are essential for structuring and managing files, with the operating system (OS) mapping logical files to physical storage (e.g., memory addresses, disk sectors, or cloud resources). Through these mappings, file systems define rules for reading, writing, and maintaining data on storage devices.

12.3 File Attributes

Files are typically characterized by the following attributes:

- **Name:** A mnemonic identifier for referencing files. Older systems, like DOS, had an 8+3 character naming format, which modern OS no longer limit.

- **Type:** Indicates the file category, often determined by a **"magic number"**: few bytes at the start of the file. Windows OS, however, may rely on extensions to associate files with applications, but for analysis is better referring to the magic number.
- **Protection:** Access control information varies across OS, specifying ownership and permissions (e.g., read, write, execute permissions on Unix systems).
- **Location:** The physical or logical storage location.
- **Size:** Specifies the file's storage size.

12.4 File System Formatting

File system formatting is the process that prepares a mass storage device for data storage by configuring it with specific file system structures. This operation is essential for organizing data storage, defining how files will be written, stored, and accessed on a storage medium.

- **Data Erasure:** Formatting typically erases existing information on the storage device.
  - **Full Formatting:** This is a slower process that erases all sectors by writing zeros across the storage and identifies any bad sectors, marking them as unusable.
  - **Quick Formatting:** A faster alternative that only erases the file system tables, leaving the actual data sectors untouched.
- **Partitioning:** Formatting can create one or more partitions on the storage device. Each partition can function as a separate logical volume, with primary, extended, or logical partitions.
- **File System Selection:** During formatting, a specific file system is selected based on the operating system requirements. Common file systems include:
  - **NTFS** for Windows, **APFS** for macOS, **ext4** for Linux.
- **Foundational Structures Creation:** The formatting process also establishes essential file system structures. These structures enable data organization and include:
  - Root directory, FAT/Inode table, superblock/Boot sector

This formatting process is crucial for initializing a storage device, defining its structure, and ensuring compatibility with the operating system and user requirements.

12.4.1 FAT File System Example

When formatting a hard drive with a FAT file system:

- The Boot Record is created, containing information such as the OS name, disk characteristics (as bytes per sectors, sectors per cluster, root directory entry).
- The Master File Table (MFT) is established, with two copies for redundancy, detailing clusters' status (available, allocated, damaged, or used by OS files).
- A Directory Table organizes the structure of top-level files and directories.

The FAT system is noted for its portability and ease of use but lacks advanced features such as encryption and robust access controls, making it less secure.

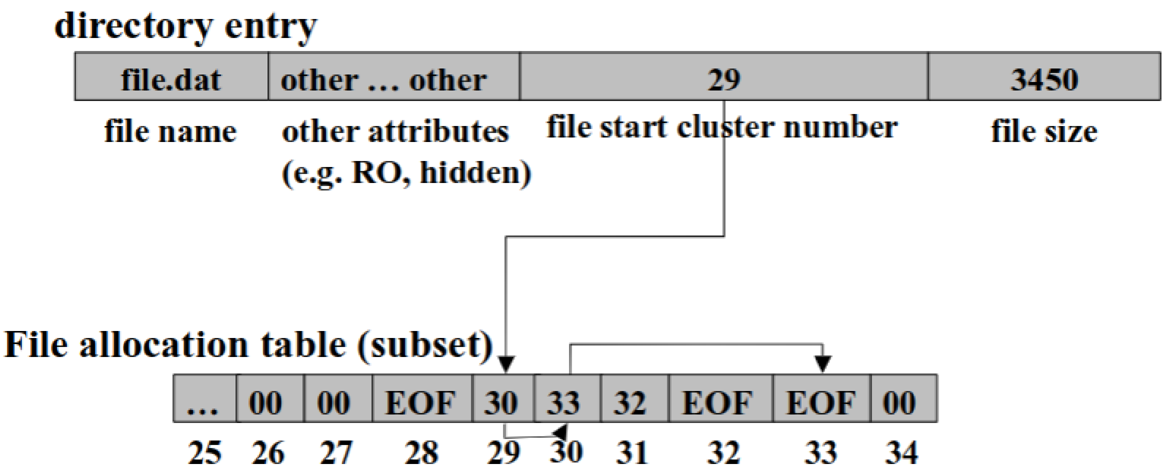


Figure 12.1: Example of a FAT File System Structure

FAT pros and cons

- portability (available to multiple operating systems)
- migration (easy switch to richer FS, like NTFS)
- fast on small volumes (some GB), due to light ”infrastructure (few metadata, no file index, ...)
- no integrated advanced features (on-the-fly compression, user quotas)
- slow for high numer of files (linked-list structure, fragmentation, no)
- no security at all (encryption, access control lists)

12.5 File Copy and Cloning

Simple file copy commands preserve file content but may alter file metadata. For forensics, bit-by-bit copies ensure fidelity to the original data, often using the `dd` command. Variants of `dd` (e.g., `dcfldd` and `dc3dd`) offer additional features like on-the-fly hashing and pattern wiping.

Example commands:

- Clone a hard drive to another: `dd if=/dev/sda of=/dev/sdb`
- Create an image file of a hard drive: `dd if=/dev/hda of=/image.img`
- Wipe a drive with binary zeros: `dcfldd pattern=00 vf=/dev/hdb`
- . . .

12.6 File Identification

File identification involves determining a file’s actual type and contents, which is crucial in forensics to verify the authenticity and integrity of data. This process often extends beyond simply looking at file extensions, as these are not a reliable source of information.

- **Limitations of Extensions:** File extensions can be easily altered by users or malicious actors, so they should not be solely relied upon to identify a file type.
- **Metadata Inspection:** Whenever possible, examine the file's metadata, as it often contains information about the file's true format and origin.
- **File Signatures:** The first few bytes of a file can act as a unique signature, known as a "magic number," which can confirm the file type. A reference list of file signatures can be found online (e.g., `https://en.wikipedia.org/wiki/List_of_file_signatures`).
- **Hex Dump Comparison:** By comparing a file's signature with its hex dump, investigators can verify the file type independently of the extension.

12.7 Metadata Example: File System

File systems maintain metadata for each file, providing critical information about its content and history. This metadata, managed by the operating system, includes:

- **File Name, Ownership, and Permissions:** Details about the file's identity, access rights, and owner.
- **Allocated Data Units:** Information on the specific data blocks or clusters assigned to the file.
- **File Size:** The size of the file in bytes.
- **Timestamps:** Key dates associated with the file, such as creation, modification, and last access times.
- **Recovery Data:** Some file systems maintain recovery information (e.g., journaling) that aids in data recovery processes.

The type and accuracy of metadata can vary significantly based on the file system in use. Common file systems with differing metadata structures include FAT32, NTFS, ext2, ext3, and ext4.

12.8 Slack Space

Slack space is residual storage within disk sectors allocated to files but not fully utilized. For example, if a 392-byte file is stored in a 512-byte sector, the remaining 120 bytes become slack space, potentially retaining data from prior file storage.

12.9 File Recovery Process

File recovery in forensics involves analyzing file system structures such as the Master File Table (MFT), which stores file metadata, including timestamps. This enables timeline reconstruction, which is crucial for investigating user actions in legal cases. Deleted files, also known as orphan files, may still be recoverable depending on the level of data overwriting and fragmentation.

12.10 Metadata Analysis in Files

Metadata, or "data about data," provides additional insights into file characteristics. Common examples include EXIF metadata for images or embedded metadata in office documents (e.g., DOCX, ODF). Metadata analysis can reveal hidden information, enhance context, and correlate data across files, though it is not inherently trustworthy and may be modified.

12.11 Data Sanitization

Data sanitization tools permanently erase data to prevent unauthorized recovery. Common methods include:

- **File Shredder Programs:** Permanently overwrite selected files.
- **Data Destruction Software:** Fully erases all data on a storage device, useful for secure disposal or virus removal.

The Air Force System Security Instruction (AFSSI) 5020 specifies a three-pass overwrite process to ensure data irretrievability.