Computer Systems Forensic Analysis AFSC

Course Presentation

Artur Varanda

School Year 2023-2024

Computer Systems Forensic Analysis:

> **Optional** – 1st year, 1st Semester – 42 hours

Lecturer:

> Artur Varanda (`artur.varanda@ua.pt`)
>
> Office hours:
>
> > send an email first to schedule a meeting (VTC)

This class aims to provide students with sound knowledge of digital forensics such as

- ✓ the collection, identification, preservation, documentation, analysis and presentation of digital evidence;

- ✓ digital evidence acquired from computers, cell phones and other electronic devices;

- ✓ this knowledge will be taught in the various areas of forensic discipline, forensic computing and forensic data analysis.

This course aims to address the transversal concepts to all areas of digital forensics such as:

- ✓ the scientific method of digital forensic investigation;
- ✓ the different types of digital forensic evidences: data, computers, mobile devices, ...
- ✓ the students will apply the knowledge acquired in the classroom to several laboratory assignments and will be able to produce a digital forensic report

Upon completion of this course, students should be able to:

- ✓ identify the different types of digital forensic evidence

- ✓ know the terminology, techniques and processes of a digital forensic investigation

- ✓ collect digital evidence from storage media

- ✓ know the limitations of digital forensics current techniques

- ✓ understand the scientific method and the need for its use

- ✓ apply the scientific method in a digital forensics investigation

- ✓ use digital some forensic tools and techniques

- ✓ comprehend forensic analysis reports

1 - **Overview of cybercrime**

- ✓ Information security principles

- ✓ AAA Services concept

- ✓ Cybercrime vs Computer Crime

- ✓ Penal framework of cybercrime

- ✓ Applicable legislation

2 - **Introduction to digital forensics**

✓ Digital investigation

✓ Digital evidence

✓ Investigation process

✓ Digital evidence handling

✓ Ethical code

3 - **Obtaining evidences**

✓ Boot process

✓ Forensic boot tools

✓ Forensic sorting tools

✓ Forensic acquisition tools

✓ *FTK Imager* overview

4 – **Data organization**

- ✓ Data storage devices
- ✓ File system analysis
- ✓ Binary and hexadecimal numbers
- ✓ Endianess
- ✓ Character encoding
- ✓ Data structures

5 -**Autopsy**

- ✓ *Autopsy* workflow
- ✓ Create cases and add data sources
- ✓ Automated processing with ingest modules
- ✓ Manual content analysis
- ✓ Report generation

6 – **Storage devices**

- ✓ Hard disk geometry

- ✓ ATA and SCSI interfaces

- ✓ Flash memory drives

- ✓ Solid State Drives (SSD)

7 – **Volumes and partitions**

- ✓ Partition tables

- ✓ Logical addresses

- ✓ Volume analysis

- ✓ Common partitions

- ✓ Volume partition tools

8 – **RAM Analysis**

- ✓ General computer architecture

- ✓ Memory acquisition tools

- ✓ Memory analysis tools

- ✓ *Volatility* overview

9 - **Mobile Forensics**

- ✓ Mobile devices

- ✓ SIM cards

- ✓ Forensic value and potential evidence

- ✓ Mobile data acquisition

- ✓ Hardware and Software tools

- ✓ *XRY* and *XAMN* overview

10 – **OSINT (Open-source Intelligence)**

- ✓ History of OSINT

- ✓ Information sources

- ✓ Information to intelligence cycle

- ✓ Open-source possibilities

- ✓ Automated processing

- ✓ Social media OSINT

- ✓ Dark Net OSINT

11 – **Documentation and Reporting**

- ✓ Physical examination

- ✓ Computer examination

- ✓ Media examination

- ✓ What to report

- ✓ Windows forensic report

- ✓ Forensic report structure

Learned knowledge will be evaluated through one individual written test and 1 team project.

Final grade = 50% Individual written test + 50% Team Project

Dates:

2023-12-16   9:00 – Individual written test

2023-12-09 23:59 – Team Project submission (Moodle)

2023-12-16 13:00 – Team Project presentation

Classes

September			
16	23	30	

October			
7	14	21	28

November			
4	11	18	25

December			
2	09	16	

Dates:

23/09/2023 – Class 1

07/10/2023 – Classes 2 and 3

21/10/2023 – Classes 4 and 5

04/11/2023 – Classes 6 and 7

18/11/2023 – Classes 8 and 9

02/12/2023 – Classes 10 and 11

16/12/2023 – Test and Team Project Presentation

EXAMS

13-01-2024	10:00	41789	ANÁLISE FORENSE DE SISTEMAS COMPUTACIONAIS	SÁBADO (SATURDAY)	FN
27-01-2024	10:00	41789	ANÁLISE FORENSE DE SISTEMAS COMPUTACIONAIS	SÁBADO (SATURDAY)	RE

Teams:
Three (3) students per Team
Exceptions must be approved by the teacher

1 week to create the teams
random pool if needed

Each team will choose just a **different** topic about digital forensic analysis:

1 - Computer Networks

2 - IoT devices

3 - Android devices

4 - RAM

5 - OSINT techniques

6 - Malicious software

7 - Dark Net

8 - Virtual Machines

Organization:
- ✓ create and discuss a plan with the team members and the teacher
- ✓ check the available resources on the Internet
- ✓ class resources will be available on Moodle

1 - Submit one PDF file, named `TeamX-report1.pdf`, with a maximum of 10 pages

write and introduction and the state of the art about the chosen topic, as well as the experimental

part, results, conclusion and bibliography with IEEE citation style.

the document should be written like a research paper:

must follow the IEEE template (A4, two columns)

2 – The PDF file will be published on Moodle for all students

3 - Prepare a presentation of up to 20 minutes

all team members must participate

present an overview of the state of the art

the presentation should focus on the experimental part, results and conclusions

Project Team Evaluation

50% – Presentation

explanation of the concepts and technical details

clarity and communications skills

argumentation in the discussion phase

50% – Report

description of concepts and procedures

expected results and tested results of forensic interest

description and usage of tools and techniques

document formatting and references

Do not commit any crime for the purpose of this project

Do not include images or videos that may violate someone's privacy

- instead, use fake images

Do not use illegal content or software to achieve your goals

Do not hack any computer without written permission

- use only virtual machines that you control and setup for this purpose

If you have any doubt about the legality of an action, ask **first**

Think thoroughly

In a real-world case, your conclusions will influence the outcome of a trial.

Write clearly

Digital forensic reports are meant to be read by nontechnical individuals:

> lawyers, judges, etc.

Always follow the digital forensics investigator code of ethics

Your team should

> split tasks among the team members in a fair way, but

> all team members have the responsibility to review the report before delivery

Software:
- Virtual machines (VMware or Virtual Box)
  - Windows and Linux VMs
- Windows Software
  - Free: FTK Imager, Autopsy 4, Volatility, XAMN Viewer

Hardware:
- Computers
  - RAM: 8GB or more recommended
  - Lots of disc space
- Large capacity USB HDD or SSD drive (≥ 250 GB)
- Low capacity USB Pen drive (≥ 8GB)
- USB, SATA and IDE write blocker (can be simulated by software)
- Camera and graduated set square (for scale purposes when taking pictures of equipment)

Main Bibliography

- Mário Antunes, Baltazar Rodrigues, Introdução à Cibersegurança - A Internet, os aspetos legais e a análise digital forense, FCA, 2018, ISBN: 978-972-722-861-4
- John Sammons, The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics, 2nd edition. Amsterdam ; Boston: Syngress, 2014.
- B. Carrier, File System Forensic Analysis, 1st edition. Boston, Mass.; London: AddisonWesley Professional, 2005.
- Cory Altheide and Harlan Carvey, Digital Forensics with Open Source Tools, 1st edition. Burlington, MA: Syngress, 2011.
- Brett Shavers, Placing the Suspect Behind the Keyboard: Using Digital Forensics and Investigative Techniques to Identify Cybercrime Suspects, 1st edition. Waltham, MA: Syngress, 2013.
- Barrett, D., & Kipper, G. (2010). Virtualization and forensics: A digital forensic investigator's guide to virtual environments. Syngress.
- Davidoff, S., & Ham, J. (2012). Network forensics: tracking hackers through cyberspace (Vol. 2014). Upper Saddle River: Prentice hall.
- Polstra, P. Linux Forensics CreateSpace Independent Publishing Platform, 2015
- Ligh, M. H., Case, A., Levy, J., & Walters, A. (2014). The art of memory forensics: detecting malware and threats in windows, linux, and Mac memory. John Wiley & Sons.
- Mahalik, H., Tamma, R., & Bommisetty, S. (2016). Practical Mobile Forensics. Packt Publishing Ltd.
- Ligh, M., Adair, S., Hartstein, B., & Richard, M. (2010). Malware analyst's cookbook and DVD: tools and techniques for fighting malicious code. Wiley Publishing.

Please Download:

"Bandido" Virtual Machine Disk   bit.ly/3Sm9QuU

Ubuntu Bionic   releases.ubuntu.com/bionic

Please Install:

VirtualBox 7.0.10   virtualbox.org

7-Zip 23.01   7-zip.org
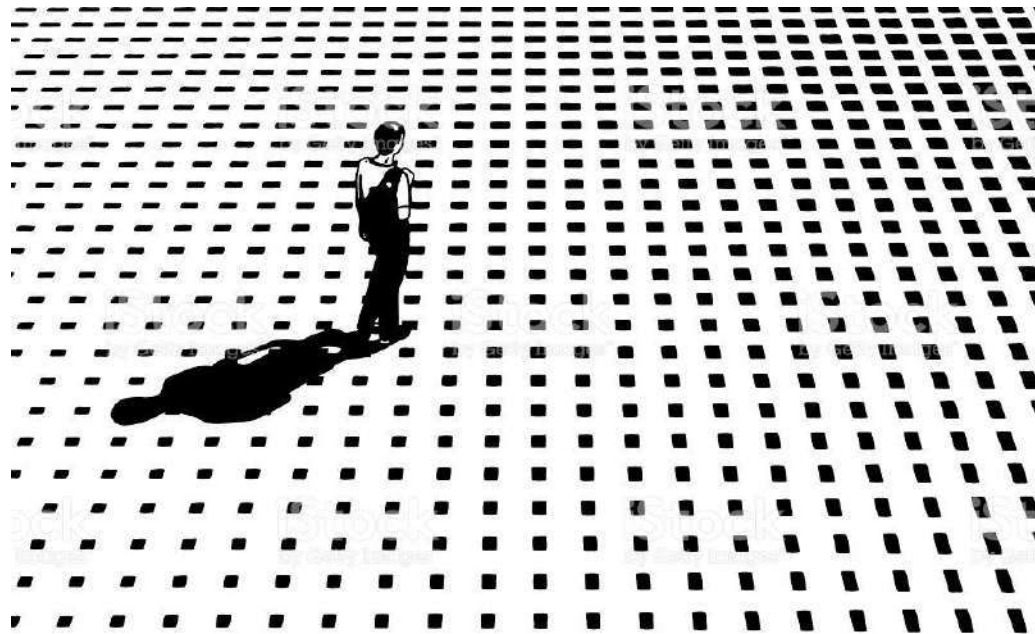
FTK Imager 4.7.0   www.exterro.com/ftk-imager

Computer Systems Forensic Analysis AFSC

1 - Overview of Cybercrime

Artur Varanda
School Year 2023-2024

Cyberspace is the human sensation of space, offered by current communication technologies, supported by new business models, social networks, cloud computing, blogs, online stores,...

Information Security Principles

The principles of information security are based on the CIA concept:

- **Confidentiality:** ensures restriction access to information;

- **Integrity:** ensures consistency and inalterability of data;

- **Availability:** ensures data availability;

Also:

- **Non Repudiation:** ensures that the sender of information is provided with proof of

  delivery and the recipient is provided with proof of the sender's identity, so neither

  can later deny having processed the information.
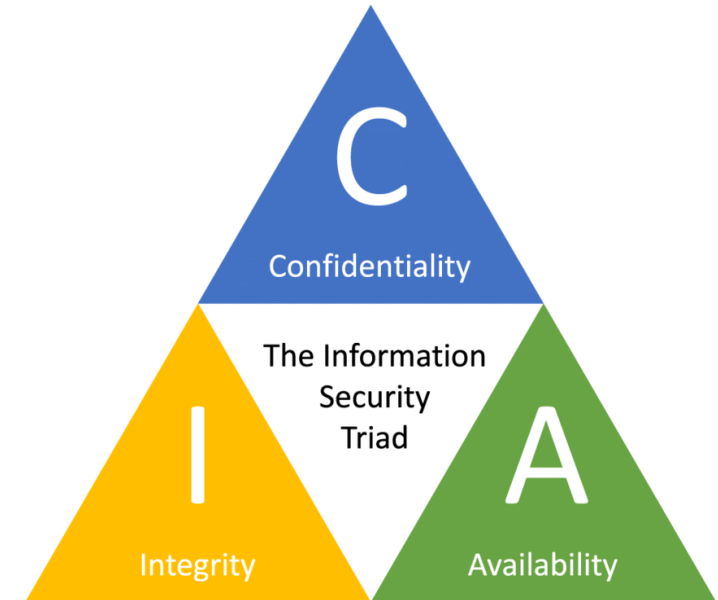
AAA Services Concept:

• **Authentication:** identity verification Ex: login and password;

• **Authorization:** user privileges;

• **Accounting:** generation of logs on user actions in the system.

Cybercrime VS Computer Crime

- Cybercrime is any illicit act practiced in cyberspace, whether it is a computer crime or any other committed by computer means.

Cybercrime VS Computer Crime

- Computer Crime – an action that violates one of the CIA or AAA principles

Cybercrime Slang

BBS's (Bulletin Board System)

Total or partial availability of information related to:
- Explosives
- Credit cards
- Description of ways to carry out crimes
- Copyright protected software

- In Portugal, BBSs are neither prohibited nor regulated, except with regard to the technical means used, which must comply with what is recommended by ANACOM – Autoridade Nacional de Comunicações.

- However, the content of BBS's and Portuguese Newsgroups cannot incite, help, facilitate or make available data or information that contravenes the law or in any way constitute a risk to personal, national or international safety.

BBS's (Cont.)

•Depending on the case, it assumes the figure of irregular practice or crime, who posts or makes available, in whole or in part, data relating to explosives, credit card numbers, description of ways of committing crimes, software protected by copyright, even if this is compressed by other programs or even if it is made available in parts or incomplete.

BlackBoxing and BlueBoxing

Blueboxing
Making unpaid phone calls using electronic devices.

Blackboxing
Interconnection of electronic components that when attached to home phones, allow all incoming calls to be received without charge to the caller.

BlackBoxing e BlueBoxing (Cont.)

Portuguese Penal Code (Decreto-Lei n.º 48/95)
Article 221
Computer and communications fraud
(Burla informática e nas comunicações)

1 - Whoever, with the intention of obtaining for himself or a third party illegitimate enrichment, causes another person to lose property, interfering with the result of data processing or by incorrectly structuring a computer program, incorrect or incomplete use of data, unauthorized use of data or intervention by any other unauthorized means of processing, is punishable by imprisonment for up to 3 years or with a fine.

2 - The same penalty applies to anyone who, with the intention of obtaining an illegitimate benefit for themselves or for a third party, causes damage to another person, using programs, electronic devices or other means that, specifically or together, are intended to reduce or change or prevent, in whole or in part, the normal operation or exploitation of telecommunications services.

Carding

•Handling and obtaining personal data from the face or from magnetic strips of credit, debit or telecommunications cards.
•All forms of data manipulation or identification elements, whether on the face or contained in magnetic strips of credit, debit or telecommunications cards, as well as the implantation of data or identification elements in other technical supports, constitute a crime of forgery, punishable by up to 3 years imprisonment.
•The use of identification elements or third-party bank details is a crime of fraud, punishable by a prison sentence of up to 3 years and is aggravated if the amount in question is high or if they continue this conduct more than once.
•Abuse of the possibility conferred by the possession of a credit card, even if only for the attempted form, is punishable by up to 3 years imprisonment, which may be aggravated up to 5 years or from 2 to 8 years, if the value is high or pretty high.

Portuguese Cybercrime Law (Lei n.º 109/2009)
Article 3
Electronic falsification
(Falsidade informática)

1 - Who, with the intention of causing deception in legal relations, introduce, modify, delete or delete computer data or in any other way interfere in the computer processing of data, producing non-genuine data or documents, with the intention that they are considered or used for legally relevant purposes as if they were genuine, is punishable by imprisonment of up to 5 years or a fine of 120 to 600 days.

2 - When the actions described in the previous number concern the data registered or incorporated into a payment bank card or any other device that allows access to a payment system or means, to a communication system or to a conditioned access service, the penalty is of 1 to 5 years in prison.
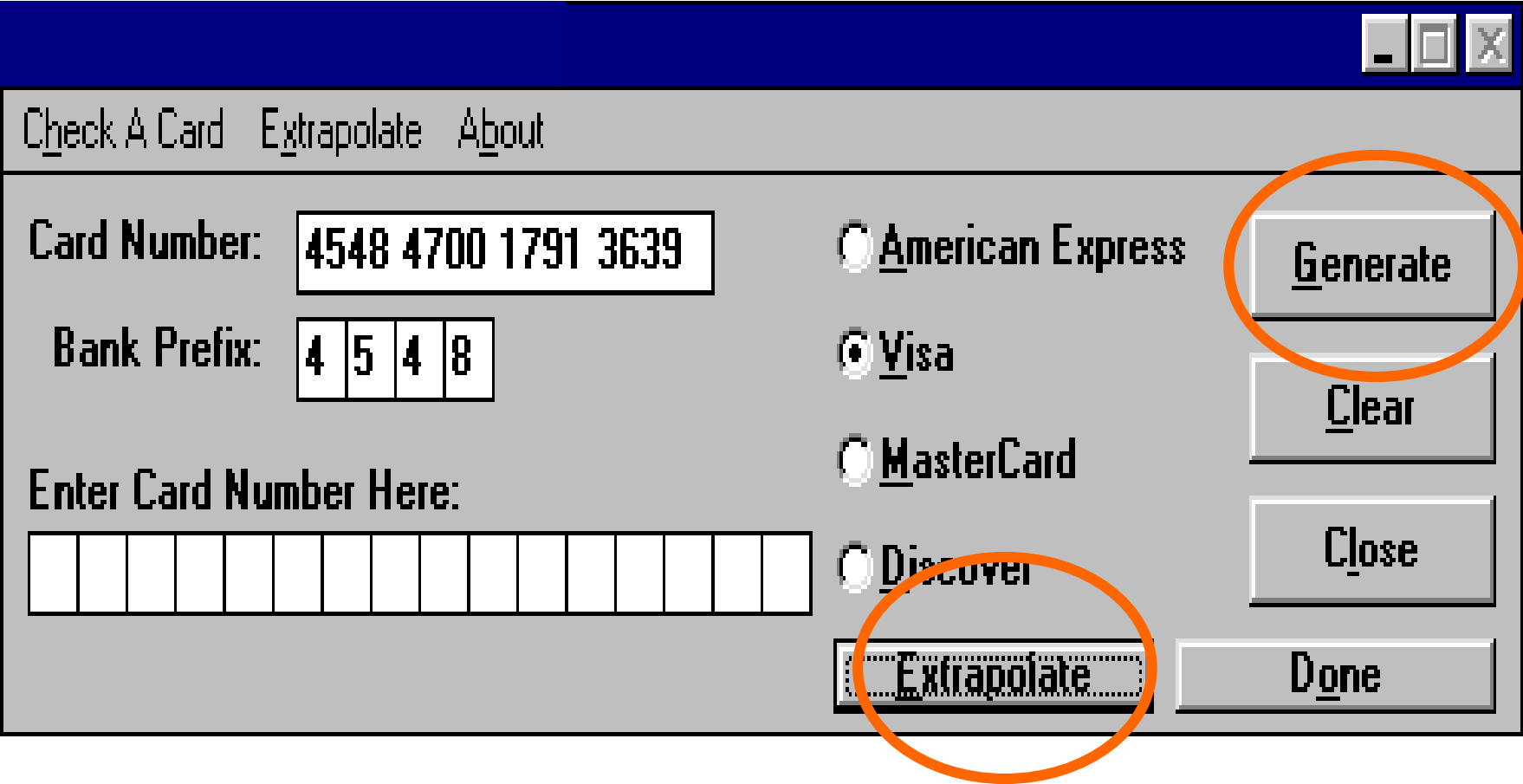
Cracking

•The process of recovering passwords from data that has been stored in or transmitted by a computer system in scrambled form.

•Modification of software to remove or disable features which are considered undesirable to the cracker, especially copy protection systems or software annoyances, like adware.

•A cracker uses the capabilities to his own advantage while belittling damages to third parties

•The [decompilation](#) of programs is punished by the Legal Protection of Computer Programs Law and by the Portuguese Cybercrime Law, by the article 8 on [illegitimate reproduction of protected program](#).

•This legislation covers memory resident programs (TSRs), which allow the use of utility software and games in violation of copyright.

Legal Protection of Computer Programs Law (Decreto-Lei n.º 252/94)
Article 7
Decompilaton
(Descompilação)

1 - The decompilation of the parts of a program necessary for the interoperability of this computer program with other programs is always lawful, even if it involves operations provided for in the previous articles, when it is the indispensable way to obtain the information necessary for such interoperability.
2 - The holder of the user license or another person who can lawfully use the program, or persons authorized by them, have the legitimacy to carry out the decompilation, if this information is not readily and quickly available.
3 - Any stipulation contrary to the provisions of the previous numbers is null and void.
4 - The information obtained cannot:
a) Be used for an act that infringes copyright on the originating program;
b) Damaging the normal exploitation of the originating program or causing unjustified harm to the legitimate interests of the holder of the right;
c) Be communicated to others when not necessary for the interoperability of the independently created program.
5 - The program created under the terms of subparagraph c) of the previous number cannot be substantially similar, in its expression, to the original program.

Portuguese Cybercrime Law (Lei n.º 109/2009)
Artigo 8.º
Illegitimate reproduction of protected program
(Reprodução ilegítima de programa protegido)

1 - Anyone who illegitimately reproduces, discloses or communicates to the public a computer program protected by law is punishable with up to 3 years imprisonment or a fine.
2 - Those who illegitimately reproduce a topography of a semiconductor product or who commercially exploit or import, for these purposes, a topography or a semiconductor product made from that topography are incurred in the same penalty.
3 - The attempt is punishable.

Hacking

•Intrusion on computer systems in order to understand how they work and gain more knowledge about it.

•A **hacker** is a computerized intellectual who loves to break into other people's systems to simply fill his ego.

•**Hackers** do not destroy, steal or spy on information for money, unlike **crackers**.

•**Cracking** activities (illegitimate access for the purpose of data destruction) are, under Portuguese law, a crime of <u>illegitimate access</u>.

Portuguese Cybercrime Law (Lei n.º 109/2009)
Article 6
Illegitimate access
(Acesso ilegítimo)

1 - Anyone who, without legal permission or without being authorized by the owner, by another holder of the right to the system or part of it, in any way access a computer system, is punished with up to 1 year imprisonment or with a fine up to 120 days.
2 - The same penalty is incurred by anyone who illegitimately produces, sells, distributes or otherwise disseminates or introduces in one or more computer systems devices, programs, an executable set of instructions, a code or other computer data intended to produce the unauthorized actions described in the previous paragraph.
3 - The penalty is imprisonment for up to 3 years or a fine if the access is gained through violation of security rules.
4 - The penalty is imprisonment from 1 to 5 years when :
a) Through access, the agent has become aware of commercial or industrial secret or confidential data, protected by law; or
b) The benefit or equity advantage obtained is of a considerably high value.
5 - The attempt is punishable, except in the cases provided for in paragraph 2.
6 - In the cases provided for in paragraphs 1, 3 and 5, the criminal procedure depends on a complaint.

General Data Protection Regulation (GDPR) **(Lei n.º 58/2019)**
Article 47
Improper access
(Acesso indevido)

1 - Anyone who, without proper authorization or justification, accesses personal data in any way is punishable with a prison sentence of up to 1 year or a fine of up to 120 days.
2-the penalty is doubled in its limits when dealing with personal data referred to in articles 9 and 10 of the GDPR.
3 - The penalty is also increased to double its limits when accessing:
a) Is achieved through violation of technical safety rules; or
b) Has provided the agent or third parties with a benefit or equity advantage.

General Data Protection Regulation (GDPR) **(Lei n.º 58/2019)**
Article 48
Data deviation
(Desvio de dados)

1 - Anyone who copies, subtracts, assigns or transfers, for a consideration or free of charge, personal data without legal provision or consent, regardless of the purpose pursued, is punishable with a prison sentence of up to 1 year or a fine of up to 120 days.
2-the penalty is doubled in its limits when dealing with personal data referred to in articles 9 and 10 of the GDPR.
3 - The penalty is also increased to double its limits when accessing:
a) Is achieved through violation of technical safety rules; or
b) Has provided the agent or third parties with a benefit or equity advantage.

General Data Protection Regulation (GDPR) **(Lei n.º 58/2019)**
Article 49
Data tampering or destruction
(Viciação ou destruição de dados)

1 - Anyone who, without proper authorization or justification, deletes, destroys, damages, hides, suppresses or modifies personal data, making them unusable or affecting their potential for use, is punishable with imprisonment for up to 2 years or with a fine up to 240 days.
2 - The penalty is doubled in its limits if the damage produced is particularly serious.
3 - In the situations provided for in the preceding paragraphs, if the agent acts negligently, he is punished with imprisonment:
a) Up to 1 year or a fine of up to 120 days, in the case provided for in paragraph 1;
b) Up to 2 years or a fine of up to 240 days, in the case provided for in paragraph 2.

General Data Protection Regulation (GDPR) **(Lei n.º 58/2019)**
Article 50
Entering false data
(Inserção de dados falsos)

1 - Anyone who enters or facilitates the entry of false personal data, with the intention of obtaining undue advantage for himself or a third party, or to cause harm, is punishable with a prison sentence of up to 2 years or a fine of up to 240 days.
2 - The penalty is doubled in its limits if the insertion referred to in the previous number results in an effective loss.

VUI's e NUI's (Virtual User Interface e Network User Identification)

•Improper use of the so-called NUIs and VUIs to access x.25 networks is a crime of <u>illegitimate access</u>, punishable by the Portuguese Cybercrime Law.

Nuke

•Name given to programs that prematurely terminate a TCP/IP connection by sending ICMP packets with error messages. Such packages can be directed to the server (server-side nuke) or to the client (client-side nuke).

Phreaking

•Act of circumventing public telephones, copying telephones, tapping and even breaking into telephone exchanges by individuals with high knowledge of telephone systems (***Phreakers***).

Phreaking (Cont.)

•In addition to applying the same principles relating to blueboxing activities, the use of communication networks based on the manipulation of telephone exchanges accessed without authorization for that purpose, constitutes the crime of <u>illegitimate access</u> under the Portuguese Cybercrime Law.

Sniffing

•Act of listening to or intercepting other people's communications.
•It is generally used to discover passwords.
•It falls under the crime of illegitimate interception.
•The trafficking of wiretapping instruments is also a crime.

Portuguese Cybercrime Law (Lei n.º 109/2009)
Article 7
Illegitimate interception
(Interceção ilegítima)

1 - Whoever, without legal permission or without being authorized by the owner, by another holder of the right to the system or part of it, and through technical means, intercept transmissions of computer data that take place within a computer system, the he intended or derived from it, is punishable with up to 3 years imprisonment or with a fine.
2 - The attempt is punishable.
3 - Incurs the same penalty provided for in paragraph 1 anyone who unlawfully produces, sells, distributes or in any other way disseminates or introduces in one or more computer systems devices, programs or other computer data intended to produce the unauthorized actions described in the same paragraph.

Portuguese Penal Code (Decreto-Lei n.º 48/95)
Article 276
Telephone tapping instruments
(Instrumentos de escuta telefónica)

Anyone who imports, manufactures, stores, buys, sells, assigns or acquires for any reason, transports, distributes or holds an instrument or apparatus specifically intended for the assembly of telephone tapping, or for the violation of correspondence or telecommunications, outside the legal conditions or otherwise according to the provisions of the competent authority, he is punishable with a prison sentence of up to 2 years or a fine of up to 240 days.

Spam

•It consists of sending a large number of unsolicited e-mal messages.

•E-mails to publicize products and services, requests for donations of assistance works, lucky chains, proposals to earn easy money, lying rumors, among others.

•Basically, it is the simultaneous sending of an e-mail message to several users at the same time. It generally has the following characteristics:
•a) is not requested by the recipient;
•b) the sender's identification is false;
•c) a victim's email server machine is used, be it an ISP or a public or private entity.

Spam (Cont.)

•In Portugal, it is this third paragraph c) that gives the criminal classification to those who send "spam", since those who use a third-party email server in those terms can be accused of committing the crime of [illegitimate access](#).

•The crime of [Electronic falsification](#) may also coexist if the falsified address identification referred to in paragraph b) (sender's identification is false) belongs to a specific person.

•If the purpose of "spam" is to interfere with the normal functioning of a computer system, it may be considered a crime of [computer sabotage](#), punishable by a five-year prison sentence or a fine.

Portuguese Cybercrime Law (Lei n.º 109/2009)
Article 5
Computer sabotage
(Sabotagem informática)

1 - Whoever, without legal permission or without being authorized by the owner, by another holder of the right to the system or part of it, hinders, prevents, interrupts or seriously disturbs the operation of a computer system, through the introduction, transmission, deterioration , damage, alteration, deletion, impediment of access or deletion of programs or other computer data or any other form of interference in a computer system, is punishable with a prison sentence of up to 5 years or a fine of up to 600 days.

2 - The same penalty is incurred by anyone who illegitimately produces, sells, distributes or in any other way disseminates or introduces into one or more computer systems devices, programs or other computer data intended to produce the unauthorized actions described in the preceding paragraph.

Phishing

•It is an attempt to trick Internet service users into providing their confidential information, such as the username and password to access Home Banking.

•Often, these attempts use apparently legitimate emails or instant messages, combined with fake websites, to make fraudulent requests for information (ie, they will "fish" data).

•Phishing is a type of online fraud and phishers are nothing less than tech savvy crooks. In a typical phishing scam, phishers send emails that appear to come from a legitimate company in an attempt to trick users into providing their personal information, which will be used for "identity theft".

•Phishers use a variety of sophisticated devices to get the information they want, including pop-up windows, URL masks that simulate real web addresses, and keyboard action readers (keyLoggers, AxisLoggers, ScreenLoggers) that capture account names and passwords.

Social engineering: Electronic falsification

Phishing email dissemination; Hosting of Phishing sites; Aggregation of information collected in Phishing scams.

Intrusion: Illegitimate access

Exploits; SQL Injections; XSS; File Inclusion; Illegal login (Brute-force; Password cracking; Dictionary attacks); Bypass control system. Theft of access credentials.

Pharming

•It is an attempt to deceive Internet users by misappropriating or misusing a website's domain name or URL and redirecting its visitors to a fake website where fraudulent requests for information are made.

•Phishing and pharming activities are punishable in Portugal, depending on the applicable legal framework, such as Illegitimate access or computer sabotage crimes under the Portuguese Cybercrime Law and also as computer and communications fraud under the Portuguese Penal Code.

Internet Grooming

•Internet grooming is the English expression used to generically define the process used by sexual predators on the Internet, ranging from initial contact to sexual exploitation of children and young people.

•It is a complex, carefully individualized process, patiently developed through assiduous and regular contacts developed over time and which may involve flattery, sympathy, offering gifts, money or supposed modelling work, but also blackmail and intimidation.

•It is, in most situations, the preparatory act for another illegal activity: **Child Sexual Abuse (Pedophilia)**

Portuguese Penal Code (Decreto-Lei n.º 48/95)
Article 171
Exhibitionist acts
(Atos exibicionistas)

Anyone who harasses another person, performing exhibitionist acts in front of him or her, is punishable with up to 1 year imprisonment or a fine of up to 120 days.

Article 172
Child sexual abuse
(Abuso sexual de crianças)

3 - Who:
a) Carrying out an exhibitionist act in front of children under 14 years of age; or
b) Acting on a minor under the age of 14, through obscene conversation or writing, pornographic performance or object, or using it in pornographic photography, film or recording;
is punishable with up to 3 years imprisonment.
4 - Anyone who performs the acts described in the preceding paragraph with a profit motive is punishable by imprisonment from 6 months to 5 years.

Portuguese Penal Code (Decreto-Lei n.º 48/95)
Article 173
Sexual abuse of adolescents and dependents
(Abuso sexual de adolescentes e dependentes)

2 - Anyone who performs an act described in the paragraphs of paragraph 3 of article 172, in relation to a minor included in the paragraphs of the previous paragraph of this article and under the conditions described therein (*), shall be punished with up to 1 year imprisonment.

3 - Anyone who practices or takes to practice the acts described in the previous number with profit intention is punishable with up to 3 years imprisonment.

(*) A minor between 14 and 16 years of age who has been entrusted with education or assistance; or a minor between 16 and 18 years of age who has been entrusted with education or assistance, with abuse of the function he or she holds.

Portuguese Penal Code **(Decreto-Lei n.º 48/95)**
Article 176
Children's pimping
(Lenocínio de menor)

1 - Anyone who encourages, favors or facilitates the exercise of prostitution of minors between 14 and 16 years of age, or the practice of relevant sexual acts, is punishable with imprisonment from 6 months to 5 years.

2 - If the agent uses violence, serious threat, ruse or fraudulent maneuver, acts professionally or with profit intention, or takes advantage of the victim's psychological incapacity, or if the victim is under 14 years of age, he is punished with a prison sentence of 2 to 10 years.

Sextortion

•Sextortion is a form of blackmail where someone threatens to share intimate images online unless the victim give in to their demands.

•These demands are typically for money, more intimate images or sexual favors.

•Blackmailers often target people through dating apps, social media, webcams or adult pornography sites.

Portuguese Penal Code (Decreto-Lei n.º 48/95)

Article 222	**Article 153**	**Article 154**	**Article 155**
Extortion	**Threat**	**Duress**	**Severe duress**
(Extorsão)	**(Ameaça)**	**(Coação)**	**(Coação grave)**

Portuguese Penal Code (Decreto-Lei n.º 48/95)
Article 222
Extortion

1 - Whoever, with the intention of obtaining for himself or for a third-party illegitimate enrichment, constrains another person, through violence or threat with important harm, to a patrimonial disposition that entails, for him or for others, damage is punishable with the penalty of imprisonment for up to 5 years.

2 - If the threat consists in the disclosure, through the media, of facts that could seriously damage the reputation of the victim or another person, the agent is punished with imprisonment from 6 months to 5 years.

Datajacking / Ramsomware

•Extortion of companies through the action of a hacker who after illegally access the system of that company proceeds to the encryption of the data stored there.

•The company is then contacted, and a ransom is required so that they can regain access to the system and information.

•It is punished in Portugal, depending on the applicable legal framework, as a crime of illegitimate access or computer sabotage under the Portuguese Cybercrime Law and as a **document extortion** under de Portuguese Penal Code.

Portuguese Penal Code (Decreto-Lei n.º 48/95)

Article 223

Document extortion

(Extorsão de documento)

Anyone who obtains, as a guarantee of debt and abusing another person's situation of need, a document that could give rise to criminal proceedings, is punishable with a prison sentence of up to 2 years or a fine of up to 240 days.

IP spoofing

•It is a computer systems subversion technique that consists of masking (spoof) IP packets using spoofed sender addresses.

•In the IP protocol, the forwarding of packets is based on a very simple premise: the packet must go to the recipient (destination-address) and there is no verification of the sender — there is no validation of the IP address nor its relationship with the previous router (who forwarded the package). Thus, it becomes trivial to spoof the source address through simple manipulation of the IP header.

•In Portugal, it can be penalized as a crime of Electronic falsification under the Portuguese Cybercrime Law or as a computer and communications fraud under the Portuguese Penal Code.
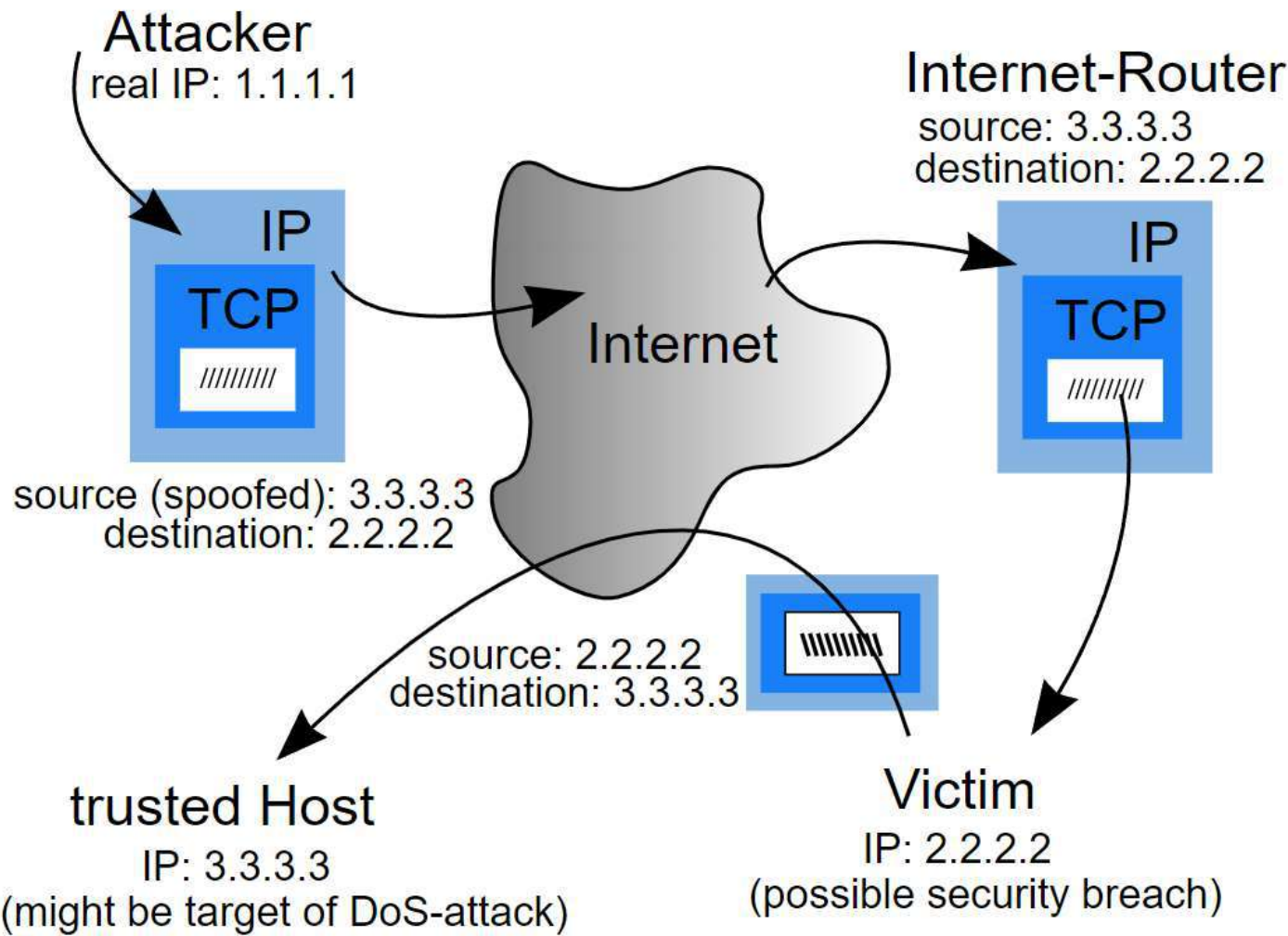
SYN flood (Denial of Service – DoS or DDoS)

- SYN attack is a form of denial-of-service attack on computer systems, in which the attacker sends a sequence of SYN (synchronization) requests to a target system.

- When a client tries to initiate a TCP connection with a server, the client and server exchange a series of messages, which are typically:

  1. The client requests a connection by sending a SYN (synchronize) to the server.

  2. The server confirms this request by sending a SYN-ACK back to the client.

  3. The client in turn responds with an ACK, and the connection is established.

- This is called the Three-Way Handshake.

SYN flood (Cont.)

Normal Connection *(TCP 3-Way Handshake)*
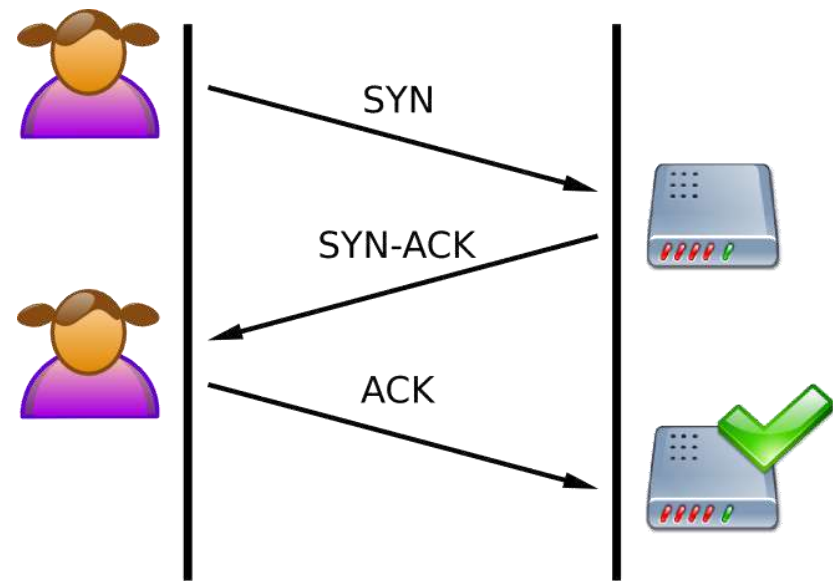
SYN Flood Attack
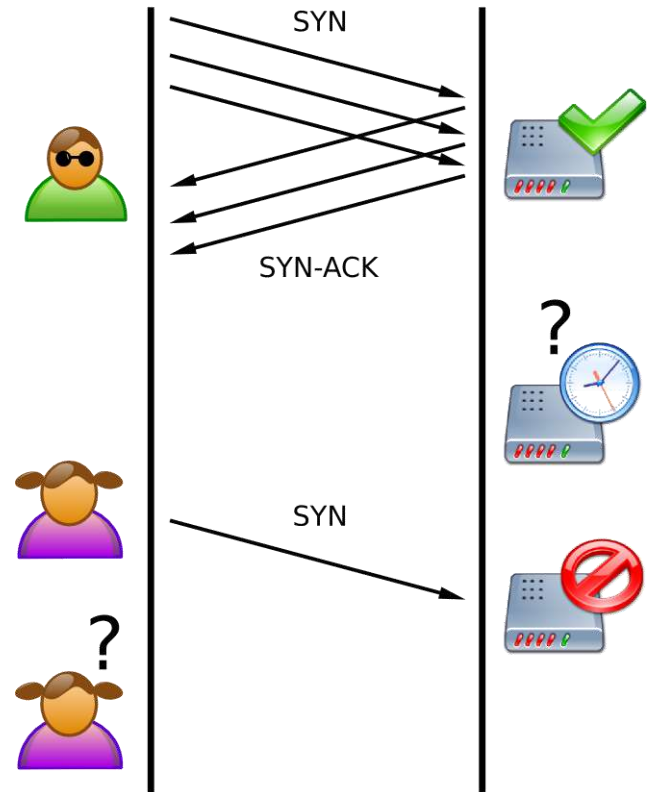
SYN flood (Cont.)

• A malicious client may not send this last ACK message.

• The server will wait for this for a while, as simple network congestion can be the cause of the missing ACK.

• This so-called semi-open connection can take up resources on the server or cause losses for companies using licensed software per connection.

• It might be possible to occupy all the resources of the machine, with several SYN packages.

• Once all resources are occupied, no new connections (legitimate or otherwise) can be made, resulting in a denial of service.

• It is penalized as a crime of computer sabotage under the Portuguese Cybercrime Law.

Cyberterrorism

•Cyberterrorism is the use of the Internet to conduct violent acts that result in, or threaten, the loss of life or significant bodily harm, in order to achieve political or ideological gains through threat or intimidation.

•The 2007 cyberattacks on Estonia were a series of cyberattacks which began on 27 April 2007 and targeted websites of Estonian organizations, including Estonian parliament, banks, ministries, newspapers and broadcasters. Most of the attacks that had any influence on the general public were distributed denial of service type attacks ranging from single individuals using various methods like ping floods to expensive rentals of botnets usually used for spam distribution.

•Stuxnet is a malicious computer worm first uncovered in 2010 and thought to have been in development since at least 2005. Stuxnet targets supervisory control and data acquisition (SCADA) systems and is believed to be responsible for causing substantial damage to the nuclear program of Iran. Although neither country has openly admitted responsibility, the worm is widely understood to be a cyberweapon built jointly by the United States and Israel in a collaborative effort known as Operation Olympic Games

•In late November 2014, Sony Pictures Entertainment was hacked by a group calling itself the Guardians of Peace. The hackers, who are widely believed to be working in at least some capacity with North Korea, stole huge amounts of information off of Sony's network.

Malware : Crime of computer sabotage under the Portuguese Cybercrime Law.

Infection; Dissemination; Web hosting or Server; Replication.

Non-availability and sabotage: Crime of computer sabotage under the Portuguese Cybercrime Law.

DoS; Disruption of processing and response capacity; Package Flood; Exploit;

Illicit information collection: Crime of illegitimate interception under the Portuguese Cybercrime Law.

Scan; Probe to system; Network scan; DNS zone transfer; Sniffing; Wiretapping

Smurf Attack

•Like the SYN flood attack, although it involves a forged ICMP (Ping Service Protocol) packet sent to a broadcast address, targeted to most operating systems and routers.

•The Smurf attack is a category of network-level attacks perpetrated against hosts with the aim of denying services.

•The attacker sends large amounts of ICMP traffic echo requests (ping) to a network broadcast IP using a source address (spoofed IP) of the victim.

•In a multi-access broadcast network, it can cause a few hundred computers on the network to respond to the request for each packet, which causes the computers on the network to bombard the victim with a response to the forged request.

•The Fraggle attack is a variation of the Smurf attack that sends large amounts of UDP packets to ports 7 (Echo) and 19 (Chargen).

•Currently, the machines most affected by this type of attacks are IRC servers and their suppliers. This type of attack is penalized in Portugal just like SYN flood attacks.

Cybersquatting

•Malicious practice which consists of registering domains relating to large companies or famous people (domain name) with the intention of taking advantage of the popularity of the person or the company's trademark, also known as domain trafficking.

•Cybersquatters often register these domains before the target company, thus forcing the target company to buy the domain from them at a higher price.

•Cybersquatting comes from the term "squatting", which describes the act of occupying a space or building, abandoned or uninhabited, without permission from its legal owners.

•In some cases, the domain name is used to post derogatory comments about the target company. The legitimate company or person has no other option than to buy the domain name at ridiculously high prices.

•This practice can be penalized as extortion in the Portuguese Penal Code.

Website defacement

•Website defacement is an attack on a website that changes the visual appearance of a website or a web page.
•These are typically the work of defacers, who break into a web server and replace the hosted website with one of their own.
•It is penalized as a crime of damage relating to programs or other computer data under the Portuguese Cybercrime Law.

Portuguese Cybercrime Law (Lei n.º 109/2009)
Article 4
Damage related to programs or other computer data
(Dano relativo a programas ou outros dados informáticos)

1 - Whoever, without legal permission or without being authorized by the owner, by another holder of the right to the system or part of it, deletes, alters, destroys, in whole or in part, damages, suppresses or renders unusable or inaccessible programs or other computer data from others or in any way affecting their ability to use, is punishable with up to 3 years imprisonment or a fine.
2 - The attempt is punishable.

Warez

•Term derived from the English language, second half of the word soft**ware** in the plural, under an l33t (elitist) pronunciation: wares /ˈwɛərz/.

•It is Software that is illegally distributed over the Internet. The "Z" is purposeful, serving to indicate something that is illegal. It can also be used in other terms such as Gamez (pirated games), Romz (video games for PC through emulators, but also illegal), i.e., the term refers to the illegal trade (**piracy**) of copyrighted products used in general in the within organized groups, making use of *peer-to-peer* networks, sharing files among friends or among large groups of people with similar interests.

•Penalized in Portugal as the crime of usurpation under the Portuguese Code of Copyright and Related Rights and as a crime of illegitimate reproduction of a protected program, under the the Portuguese Cybercrime Law.

•Copying and distributing to third party computer programs protected by law - copyright - are prohibited and punishable by law up to three years in prison. Attempted copying or distribution is also punishable.

•This law covers the total or partial distribution of computer programs, even if compressed by other programs, in newsgroups, IRC's, www, ftp, etc.

Portuguese Code of Copyright and Related Rights (Decreto-Lei n.º 63/85)
Article 195
Usurpation

1 - Any person who, without authorization from the author or the artist, the producer of phonogram and videogram or the broadcasting organization, uses a work or service in any of the ways provided for in this Code, commits the crime of usurpation.
2 - Also commits the crime of usurpation:
a) Anyone who improperly discloses or publishes a work not yet disclosed or published by its author or not intended for dissemination or publication, even if it is presented as belonging to the respective author, whether or not intending to obtain any economic advantage;
b) Whoever collects or compiles published or unpublished works without the author's authorization;
c) Who, being authorized to use a work, artist, phonogram, videogram or broadcast broadcast, exceeds the limits of the authorization granted, except in the cases expressly provided for in this Code.
3 - Will be punished with the penalties provided for in article 197, the author who, having transmitted, in whole or in part, the respective rights or having authorized the use of his work in any of the ways provided for in this Code, to use it directly or indirectly with offense of the rights attributed to others.

Examples (Images)

Distribution Box

Call-box
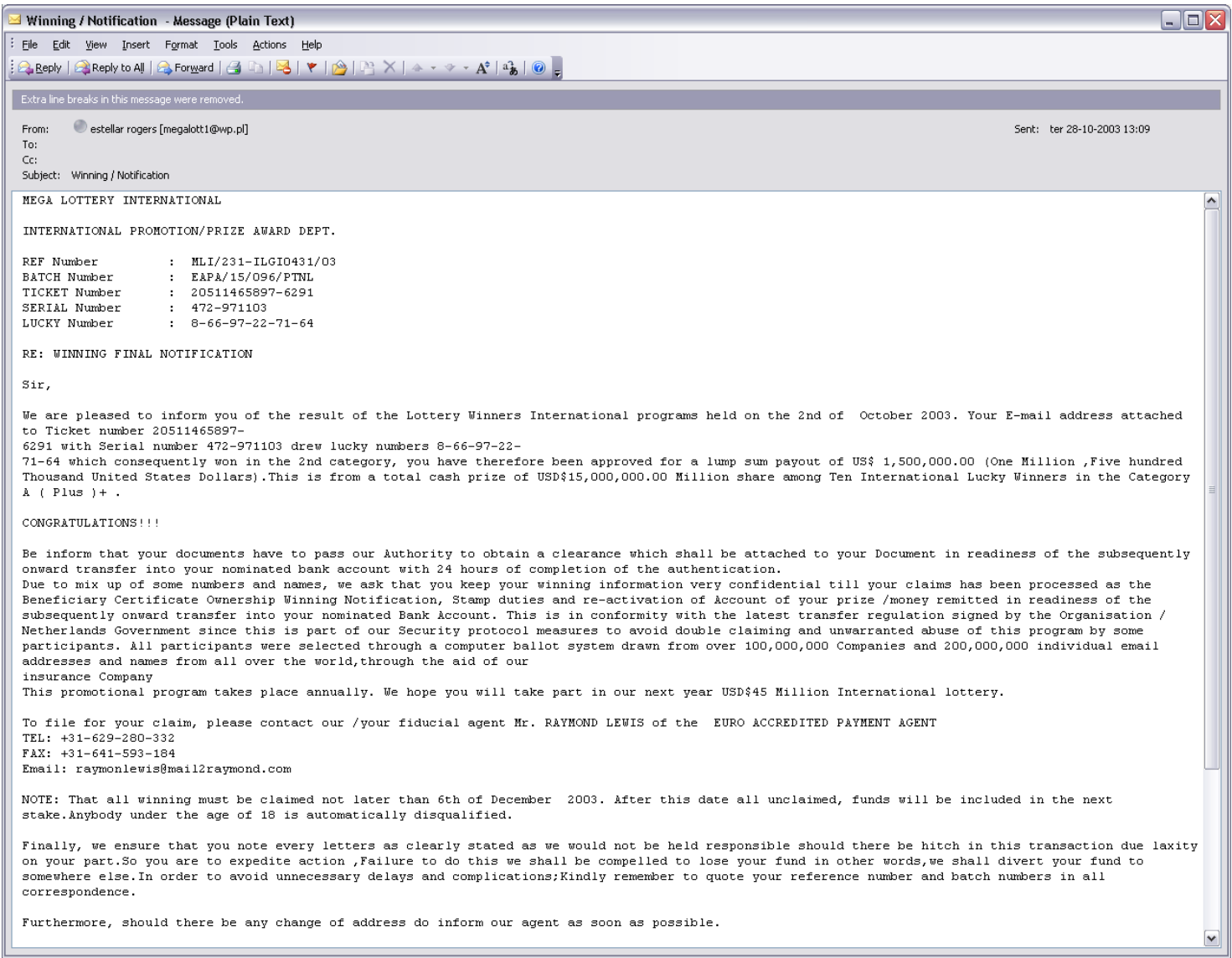
1 card type   **2.6 BIN**   **7.15 acc**   **check digit**

Track 1: Holder Name, Primary Account Number, Expiration Date, Verification Values

Track 2: Primary Account Number, Expiration Date, Verification Values

Track 3: Primary Account Number, User and Security Data, Additional Data

Examples - Phishing

Examples - Phishing

Digital Evidence

Digital evidence, like any other evidence, must be:

- **Admissible**

- **Authentic**

- **Precise**

- **Complete**

Digital Evidence - Requirements

- legally admissible
  - how it is obtained

- technically irrefutable
  - source
  - integrity
  - certification (digital signature)
  - dual control

Adapted from BLAKESLEEL, Hyechin - USE OF

COMPUTER FORENSICS TECHNOLOGIES

IN CRIME INVESTIGATION, 2009; KSANDER, 2006;

The process of a forensic analysis is divided into four stages:

1. Identify the source of the digital evidence;

2. Preserving the evidence (involves the duplication of evidence according to technical-legal processes);

3. Analysis and investigation of evidence;

4. Presentation of reports and documentation of results.

Computer Systems Forensic Analysis AFSC

Obtaining Evidences

Artur Varanda

School Year 2023-2024

- It is normal forensic practice to remove a hard drive from a computer, write-block it and then image that hard drive
- But sometimes that is not possible:
  - ✓ some thin laptops have SSD chips soldered to the motherboard
  - ✓ the storage device has a non standard data interface and the examiner doesn't have the appropriate connector:
    - in these cases the imaging of the storage device needs to be done with the drive connected to the computer;

Use a forensic boot device on the computer:

- boot diskette, bootable CD-ROM/DVD, or bootable USB device

  to ensure the storage drive is not altered either during the boot or the acquisition phase.

The normal startup of a computer alters data on the primary storage drive during the boot process

- it is required to protect the integrity of the original evidence
- we must modify the start-up process in order to prevent any changes to the data on the storage drive

Boot process
- the normal boot process begins within the computer's hardware and moves to the boot device
- there are no changes made until the computer transfers control to the boot device

Boot process steps

- most systems have 2 phases:

    1. configure and start the hardware

    2. find the operating system and run it

- boot code – machine instructions used by the computer

- when it is starting when power is applied to a CPU:

    ✓ it reads instructions from a specific location in memory – typically ROM

    ✓ the instructions in ROM force the system to probe for and configure hardware

    ✓ then searches for a device that may contain additional boot code
      - disks reserve space for boot code, but it isn't always used
      - its boot code is executed, and attempts to locate and load an operating system
      - the process after the bootable disk is found is platform-specific

Boot code characteristics

- has a specific location
- the instructions are in machine code

    0xB400   *// machine code*

    MOV AH,00 *// machine code representation in Assembly*

    on a storage device it is difficult to distinguish random data from machine code

Systems with BIOS (Basic Input/Output System):
- BIOS boots by reading the first sector on a hard disk and executing it
    which has space limitations
- this boot sector code in turn locates and runs additional code in the first sector of the partition
- which locates and loads the actual operating system

UEFI (Unified Extensible Firmware Interface)

- boots by loading EFI program files (with .efi filename extensions)
  - ✓ stored in a special disk partition, known as the EFI System Partition (ESP)
- it can read files from a partition on the hard disk
- it is not limited to the size of the first sector
- it allows booting OS on disks with more than 2TB
  - ✓ regardless of the CPU architecture
- it supports graphics user interfaces on startup
- **secure boot** – is a feature of UEFI
  - ✓ the boot code must be digitally signed to prevent the installation of malware in the boot code
  - ✓ the examiner must use a forensic boot device that supports secure boot
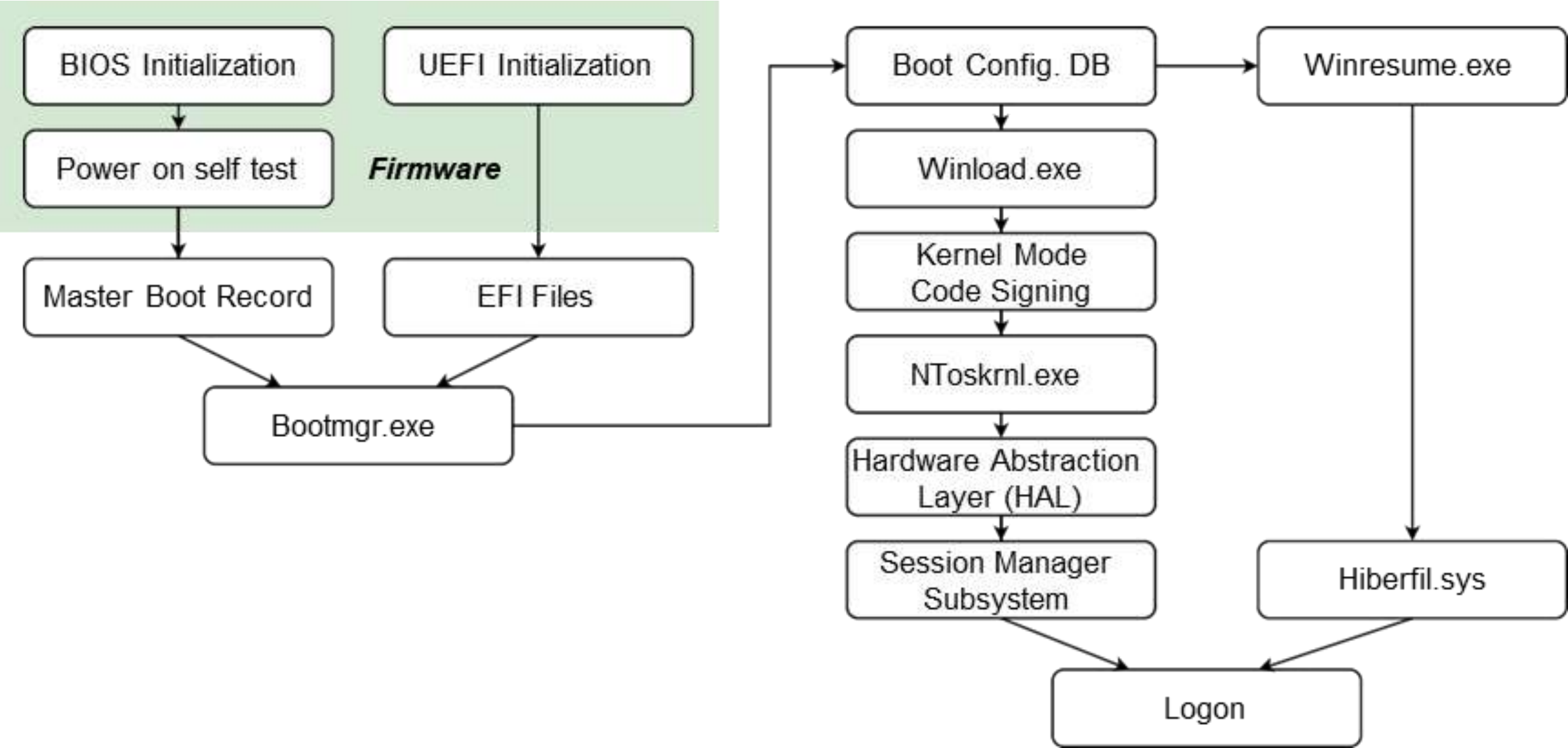
Forensic Boot Tools

DOS boot disk (obsolete, but some times required)

- there are three files required to boot a computer into MS-DOS:

  `O.SYS`, `MSDOS.SYS` and `COMMAND.COM`

- if present are also used in the boot process:

  `DRVSPACE.BIN` or `DBLSPACE.BIN`, `CONFIG.SYS` and `AUTOEXEC.BAT`

How to create a **forensic** bootable diskette:

- on the command line of Windows 98: `format a: /U /S`

  `/U` unconditional format

  `/S` copy the necessary system files over to the diskette, in order to make it a boot disk

- then remove every file from the diskette except the mandatory three (see above)

- remove special attributes from the files to be deleted: `attrib -H -R -S filename`

  later, it is possible to customize the forensic boot disk by adding `CONFIG.SYS` and `AUTOEXEC.BAT` files

  write-blocking utilities and other forensic tools

If you don't have a Windows 98 running

- HP makes an easy to use utility called HP USB Disk Format Tool, which includes a "Create a DOS Startup Disk" option

  - ✓ It's available for free download at http://www.19systems.net/HP-USB-Tool-v2.1.8.exe along with the Windows 98/DOS boot files http://www.19systems.net/Win98-Boot-Files.zip

- once the bootable diskette is created follow the same procedures to make it "forensic":

  - ✓ remove every file from the diskette except the mandatory three `O.SYS, MSDOS.SYS` and `COMMAND.COM` later, it is possible to customize the forensic boot disk by adding `CONFIG.SYS` and `AUTOEXEC.BAT` files write-blocking utilities and other forensic tools

There are many Linux based bootable CD-ROMs (or Live CDs) with forensic tools, such as:

- Paladin (www.sumuri.com) – linux distro with many forensic GUI tools, including Autopsy
- DEFT (Digital Evidence & Forensic Toolkit https://www.deftlinux.it/index.html) is a customized distribution of the Ubuntu live Linux CD
- Caine (Computer Aided INvestigative Environment https://www.caine-live.net) is an **Italian** GNU/Linux live distribution created as a Digital Forensics project (Installation and resolving Stuck Boot-Repair)
- Kali Linux (https://www.kali.org) is an open-source, Debian-based Linux distribution geared towards various information security tasks, such as Penetration Testing, Security Research, Computer Forensics and Reverse Engineering

Create a bootable CD-ROM:

- find and download the `ISO` file, *e. g.* paladin_edge_64.iso
- use a CD-burning program to write the `ISO` file to the CD

Linux based bootable CD-ROM disadvantage

Not all first responders are comfortable using Linux

There are several Windows based bootable CD-ROMs (or Live CDs):

- WinFE (Windows Forensic Environment) created by Brett Shavers – Free

- System Acquisition Forensic Environment (SAFE) Boot Disk by Forensic Soft – Commercial

- Gargoyle Investigator by Wetstone – Commercial

WinFE (https://www.winfe.net)

Advantages

- it's free, but requires a Windows license

- runs windows software, *e. g.* FTK Imager, RegRipper, . . . can be customized

Disadvantages

- requires configuration on the part of the user prior to use

- must be built to customize with your own set of tools

Nowadays, most computers don't have CD/DVD drives.

Tools to create a bootable USB device:

on Windows

- UNetBootIn (https://unetbootin.github.io/)

- Rufus (https://rufus.ie/)

on Linux

- Gnome Multi-Writer (https://gitlab.gnome.org/GNOME/gnome-multi-writer)

- Etcher – USB and SD Card Writer (https://etcher.download/)

- UnetBootIn for Linux (https://unetbootin.github.io/linux_download.html)

- DD command line tool: `sudo dd bs=4M if=input.iso of=/dev/sdx conv=fdatasync` (replace `sdx` by the drive letter of the USB device)
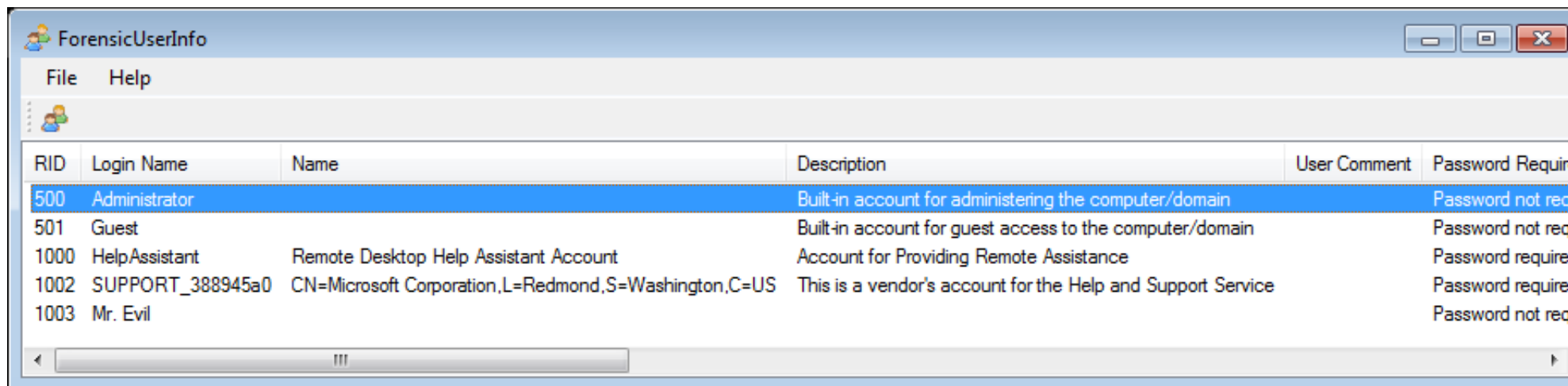
Forensic Sorting Tools

RegistryReport

- homepage: https://www.gaijin.at/en/software/downloads

- requires the `SAM`, `SOFTWARE`, `SYSTEM` and `NTUSER.DAT` registry files

- doesn't process the registry files of the running operating system

- shows information about (Windows 2000 or higher)

    ✓ the operating system

    ✓ installed software

    ✓ the last user activity

    ✓ the user settings

    ✓ and many other details

- the amount of information for each category can be configured in the settings dialog

- it allows to save, print and search the generated report

ForensicUserInfo

- homepage: https://github.com/woanware/ForensicUserInfo

- requires the `SAM`, `SOFTWARE` and `SYSTEM` files

- extracts the following information:
  - ✓ RID, Login Name, Name, Description, User Comment
  - ✓ LM Hash, NT Hash
  - ✓ Last Login Date, Password Reset Date, Account Expiry Date, Login Fail Date
  - ✓ Login Count, Failed Logins, Profile Path, Groups

Mitec WRR (Windows Registry Recovery)

- homepage: https://www.mitec.cz/wrr.html

- for crashed machine, registry configuration, data recovery

- it allows to explore:
  - ✓ File Information
  - ✓ SAM
  - ✓ Security Record Explorer
  - ✓ Windows Installation
  - ✓ Hardware
  - ✓ User Data
  - ✓ Startup Applications
  - ✓ Services and Drivers
  - ✓ Network Configuration
  - ✓ Windows Firewall Settings
  - ✓ Environment,
  - ✓ Shell Folders
  - ✓ Outlook Express,
  - ✓ Raw Data

RanSack

- homepage:

  https://www.mythicsoft.com/agentransack/
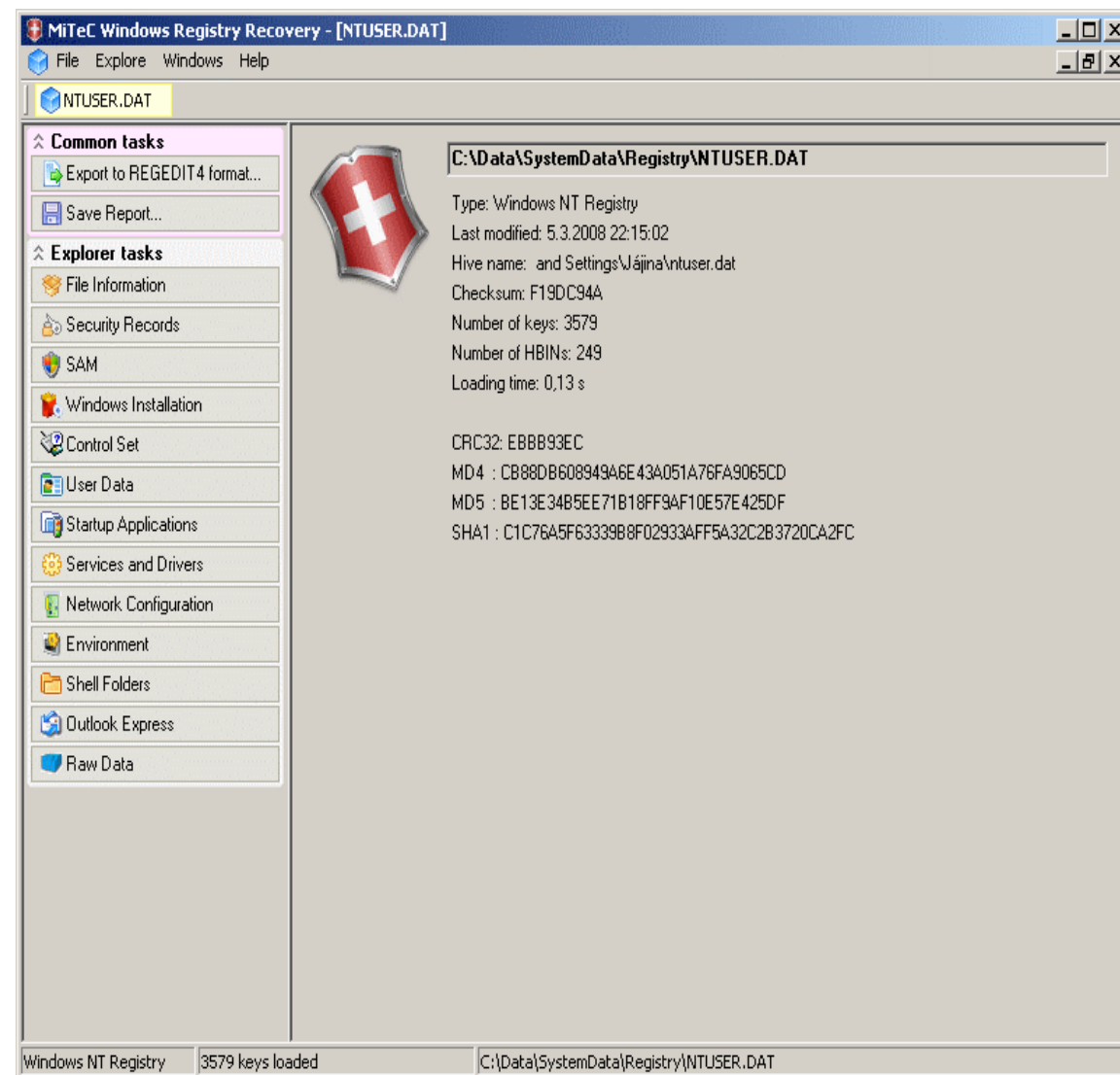
- free software program for finding files on your PC or network drives
  - ✓ fast search (less time waiting)
  - ✓ powerful search capabilities (Boolean expressions, Perl regex)
  - ✓ supports Microsoft Office and Libre Office files formats
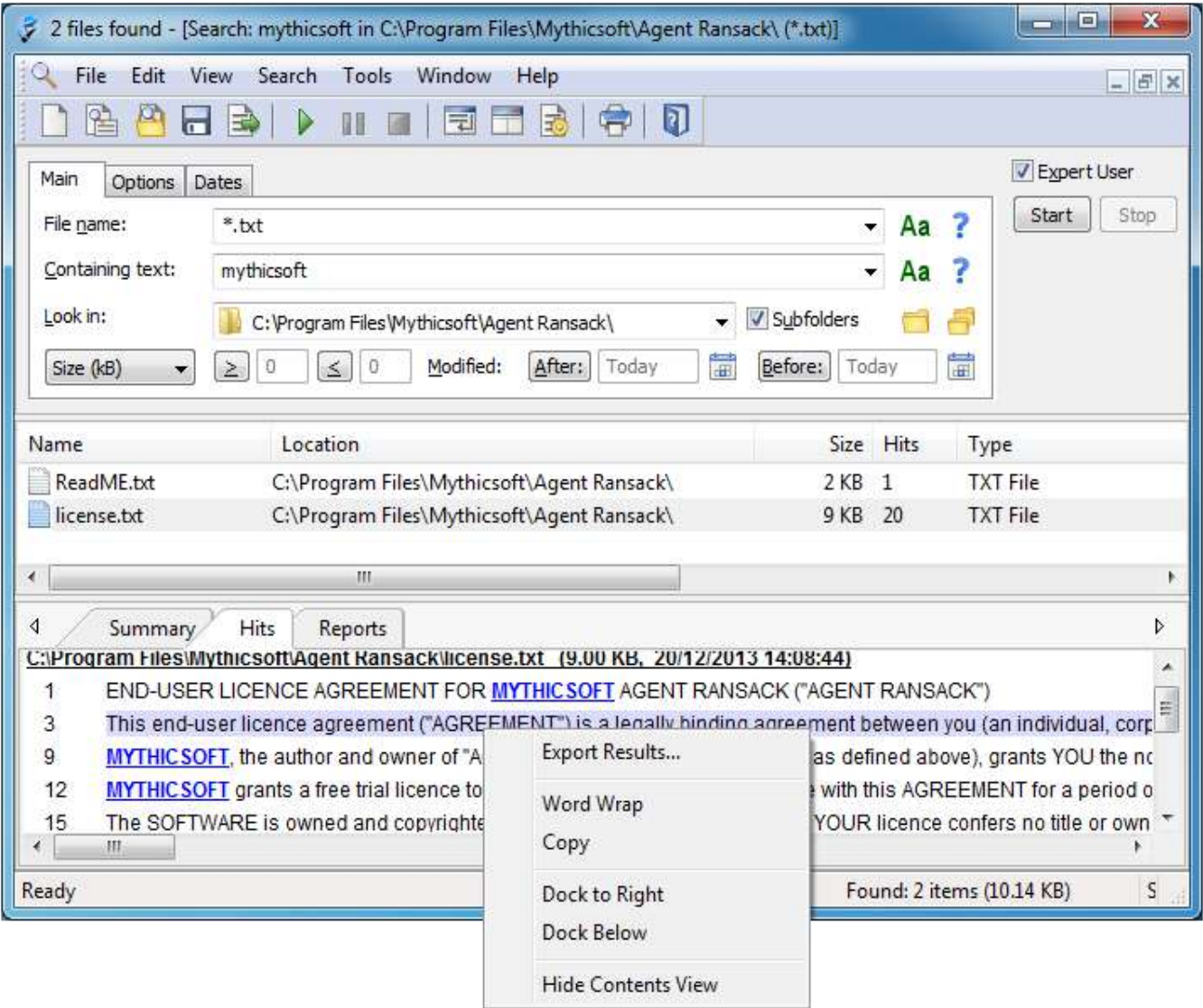
Portable Forensic Tools

- collection of freeware tools, such as:

  ✓ DataProtectionDecryptor – decrypts passwords of Microsoft Outlook accounts, credentials files of

     Windows, wireless network keys, passwords in some versions of Internet Explorer, passwords and cookies

     of Chrome Web browser

  ✓ JumpListsView – displays the information stored by the 'Jump Lists'

  ✓ Windows File Analyzer – decodes and analyzes to provide cached information

  ✓ BinText – extracts strings from binary files

  ✓ Data Converter – converts numbers, hexadecimal values or dates

  ✓ EXIF Viewer – displays EXIF informations from JPEG images

  ✓ eMule MET Viewer – shows various information from the eMule

  ✓ …

- to find more portable tools: https://www.portablefreeware.com

FTK Imager

- homepage: https://www.exterro.com/ftk-imager

- very powerful and user-friendly tool

  - ✓ runs as portable application, ideal to include in WinFE

  - ✓ search files

  - ✓ look for deleted files

  - ✓ copy files (*e. g.* cache and registry files)

  - ✓ identify ADS (Alternate Data Stream)

 - ✓ acquire storage devices and RAM

  - ✓ mount `E01` files

  - ✓ …

Forensic Acquisition

Data Acquisition

- typically occurs in the "system preservation" phase

- although it might also occur on a running system

- this is an import phase

  ✓ if not done properly data can be lost forever

  ✓ it must be done in a way that does not undermine its legal validity

What to do if:

- the computer is off → remove power cord

- the computer is on:

  ✓ take a picture of the screen

  ✓ are destructive processes running? → remove power cord

  ✓ do a memory dump and get network connections status →

    this may destroy or contaminate evidences

    - when you cannot turn off a server

    - to get passwords or encryption keys stored in RAM

    - to monitor malicious software network activities
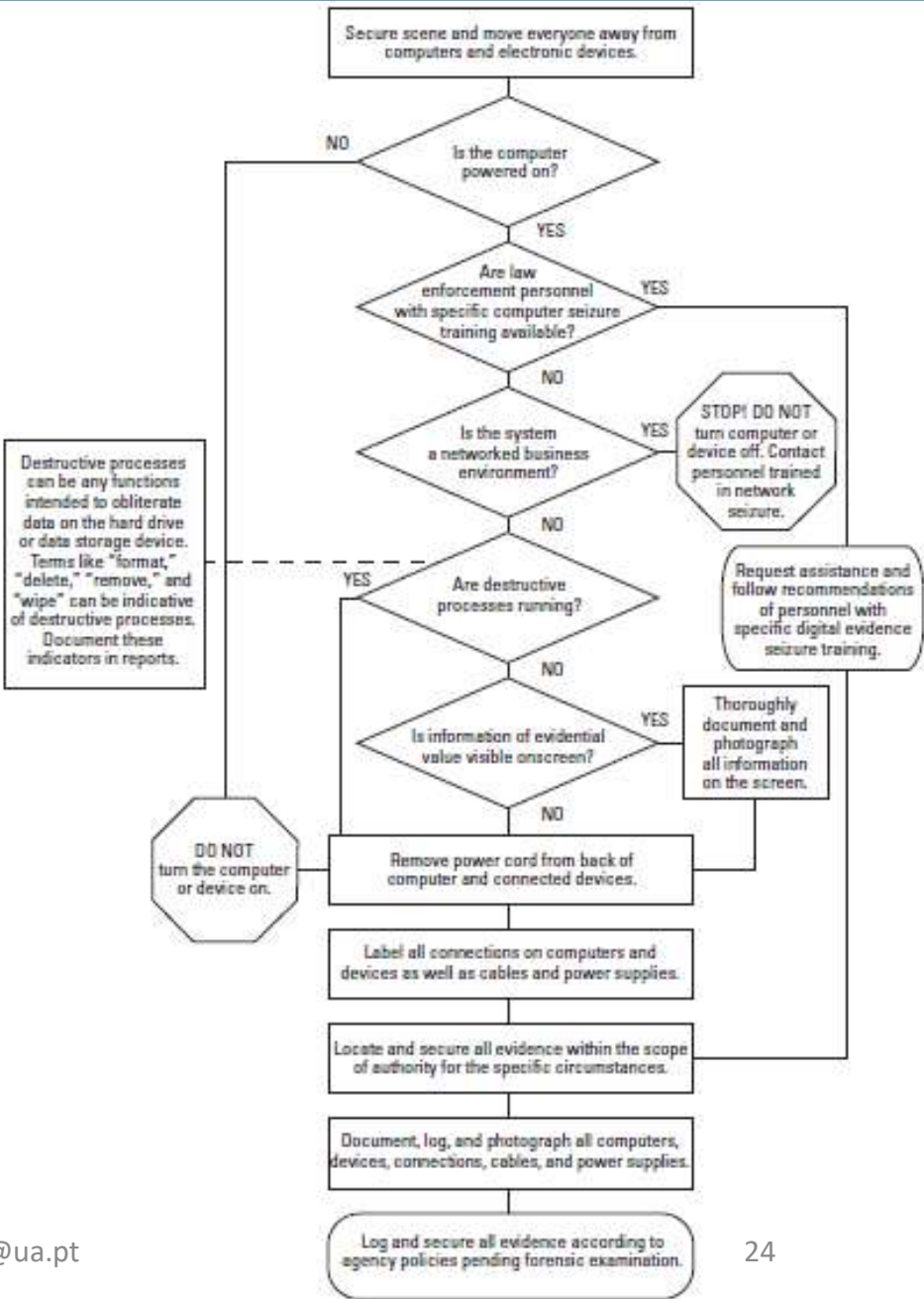
Source: Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition (U.S. Department of Justice)

Information analysis layers on storage media:

- physical – from the first to the last bit of the storage media

- volume – it is not possible to get unallocated sectors, partition table or hidden areas

- file – file copies (*e. g.* backup tools) less likely to retrieve deleted files

- application – each application has its own encoding or file format

The higher the acquisition layer, the less information can be retrieved

Whenever possible, data acquisition should be made at the physical level.

Other media:

- network and volatile memory

- each medium as its own recommend procedures

Copying storage media

- the bigger the block size, the faster the acquisition,

- but if there are sectors with errors, the all block will be invalid

- the acquisition block size should match the sector size

  - ✓ for HDD the sector size is 512 bytes

  - ✓ for SSD sector size depends on the brand, model and capacity

- data acquisition should include the complete storage medium (physical level)

  - ✓ including unallocated sectors, and

  - ✓ hidden areas: HPA or DCO – in this case 2 acquisitions are recommended

    - ▪ one with the hidden area in place, and another with the hidden areas disabled

Data acquisitions from storage media

make a storage medium forensic copy

- requires another storage medium of equal or bigger size, although many

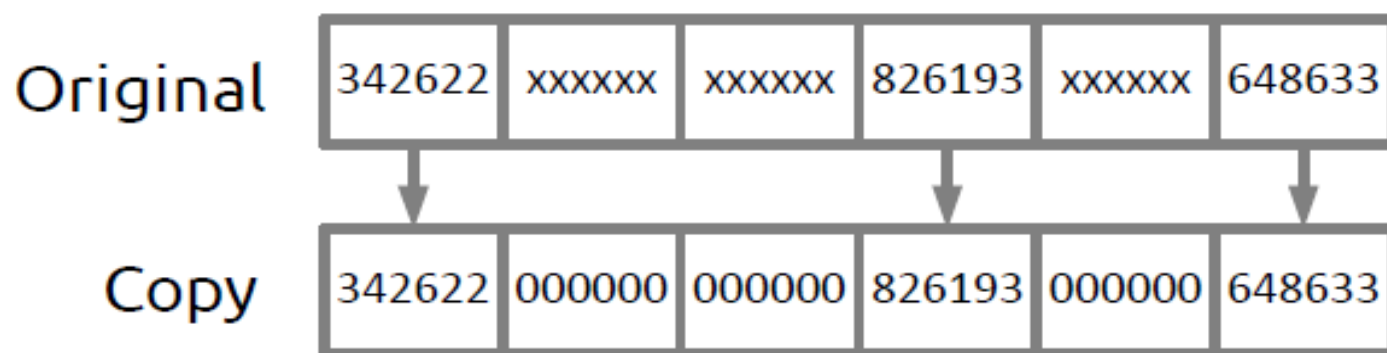   tools can create compressed images files

reading the data

- through the BIOS – old BIOS don't support large storage drives $\rightarrow$ may report wrong

    drive size

- direct access – the best choice, but not supported by all tools

Post mortem versus alive data

- acquisition post mortem

  - ✓ the OS is shutdown

  - ✓ suspect hardware can be used using a trusted OS to boot it

    - ▪ **Caution**: new PCs boot too fast and we might not be able to change boot order

  - ✓ the NSA scandal showed that we cannot always trust the hardware

    - ▪ spyware inside HDDs' firmware

  - ✓ although it is less likely to happen than software tampering

- alive

  - ✓ the OS is running and used to perform the acquisition

    - ▪ there is the risk of the OS have been tampered and return wrong data

    - ▪ *e. g.* rootkits that hide processes and files to avoid detection

  - ✓ online acquisition should be performed only in special situations

What happens if the drive has bad sectors?

- acquisitions is still possible, if the percentage of bad sectors is small

- the tool must be able to deal with the errors:
    - ✓ place zeros on the bad sectors, so the data keeps its alignment
    - ✓ otherwise the forensic copy would be smaller and the analysis tool could trigger errors
    - ✓ the tool must register in a log file all the identified bad sectors
    - ✓ tools should automatically decrease the acquisition block size to the sector size

| Original | 342622 | xxxxxx | xxxxxx | 826193 | xxxxxx | 648633 |

| Copy | 342622 | 000000 | 000000 | 826193 | 000000 | 648633 |

Host Protected Area (HPA)

- this area should be copied also, it may contain hidden data
- few tools support reading HPA
  - ✓ we can use the `hdparm` tool to temporarily access it (a reboot will restore the HPA)
  - ✓ as a precaution measure, we should make first one forensic copy with HPA in place

Device Configuration Overlay (DCO)

- the removal of the DCO is permanent, so as a precaution measure, we should make first one forensic copy with DCO in place
- few tools support reading DCO areas
  - list of tools is available in https://forensics.wiki/dco_and_hpa/ (old site)

Tableau Imager is able to identify and read both HPA and DCO

Write blockers stop any write operation to the storage media under investigation

- Hardware

  ✓ specific for each medium interface: ATA, SATA, SCSI, Firewire (IEEE 1394) or USB

  ✓ stops write operations regardless of the used OS

  ✓ specialized hardware provides better acquisition performance

  ✓ some hardware works like a proxy and monitors all operations

  ✓ this is the best option, but it is also the most expensive

  ✓ list of tests on hardware write blockers:

    - https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt/cftt-technical/hardware

- Software

  ✓ this is the less expensive solution

  ✓ but may be less effective, some apps can bypass the software write block

  ✓ list of tests on software write blockers:

    - https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt/cftt-technical/software

There are 2 main approaches to acquire data:

- cloning

  - ✓ it is recommended to use drives of the same size

  - ✓ if the clone driver is bigger, where the cloned data ends?

  - ✓ it is highly recommended to zero out first the drive before cloning

  - ✓ drive geometry of the clone might be different

  - ✓ some OS, namely Windows, by default *auto mount* drives, so you need write blockers to analyze the clones

- imaging the drive – the most common approach

  - ✓ it is not vulnerable to *auto mount* by the OS

  - ✓ an image will always be mounted as read only, no need for a write blocker

  - ✓ it is possible to simulate read/write operation

  - ✓ the changes will be stored in a cache file, leaving the original intact

  - ✓ this way one drive can store image files from several different media

  - ✓ the image file can be split into smaller files to fit in a DVD

There are several image formats for acquired data:

- *raw image* – most flexible format, supported by all analysis software

- *raw image* + external metadata – like the raw image, but adds another file with description data, hash values and time

- *embedded image* – proprietary format, the metadata is embedded inside the image

- some image file formats support compression

    - ✓ save storage space, but the acquisition process takes longer to complete

    - ✓ not all tools support compressed image files – it might be required to uncompress first

    - ✓ good solution for long term storage of the image files

Acquisition

- local acquisition – implies physical access to the storage drive

- remote acquisition

    - ✓ when it is not possible to have physical access to the storage drive

    - ✓ when there are no adequate adapters for the storage medium

    - ✓ this process is slower, usage of compression is recommended

    - ✓ if there are no full control of the network encryption should be used

To guarantee integrity, hash values should be stored

- hash blocks of small size to prevent a single error to invalidate all drive image

  - ✓ *e. g.* the same size of the acquisition block

- in a RAW file; hash values are stored in a separate file

- **It is always recommended to do a digital signature on the hash values files**

  - ✓ Why do you think this is good practice?

Digital signatures

- best tool is GnuPG - https://www.gnupg.org/

- if possible, use also a time stamping server

Tools for data acquisition on storage media there are many tools

- Windows – with graphical user interface

  ✓ FTK imager, Tableau imager, . . .(https://www.exterro.com/ftk-imager)

- Linux – many are command line

  ✓ GUI – Guymager (https://guymager.sourceforge.io/)

  ✓ CMD – ewftools, dd and derived tools: dcfldd, dc3dd, ddrescue, dd_rescue, rdd . . .

Computer Forensic Tool Testing (CFTT) project

- develops test-cases for digital forensic tools

- tests the tools and publishes the results

  https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt

Expert Witness Format (EWF)

- proprietary format from EnCase tool, supports compression

  ✓ file extension: `E01,E02,...`

- there are also <u>open-source tools</u>: `apt-get install ewf-tools`

  ✓ `ewfacquire` – acquire drive data locally

  ✓ `ewfacquirestream` – acquire drive data remotely

  ✓ `ewfmount` – mount EWF images (will be mounted as a RAW file)

  ✓ `ewfexport` – convert image file formats

  ✓ `ewfinfo` – get info from a an EWF image file

  ✓ `ewfrecover` – tries to recover corrupted `EWF` files

  ✓ `ewfverify` – validate EWF file integrity → **very important** before start an analysis

```
sudo apt install ewf-tools        # Install EWF tools
ewfexport -f raw filename.E??      # EnCase → RAW
```

Acquisition example:

```
ewfacquire /dev/sdd                                      # issued command line
ewfacquire 20130416                                      # info generated by the tool

Device information:
Bus type:
Vendor:                           ATA
Model:                            VMware Virtual I
Serial:                           00000000000000000001

Storage media information:
Type:                             Device
Media type:                       Fixed
Media size:                       53 MB (53477376 bytes)
Bytes per sector:                 512

Acquiry parameters required, please provide the necessary input
Image path and filename without extension: example         # interactive part
Case number: 001
Description: This is just a test
Evidence number: 000001
Examiner name: Miguel Frade                                # who did the acquisition
Notes: Visrtual disc drive
(...)
Compression level (none, empty-block, fast, best) [none]: best  # compress option
(...)
```

Example

- download `EWF` files:

  http://downloads.digitalcorpora.org/corpora/drives/nps-2008-m57-jean/nps-2008-jean.E01

  http://downloads.digitalcorpora.org/corpora/drives/nps-2008-m57-jean/nps-2008-jean.E02

- get info: ewfinfo nps-2008-jean.E0*

- mount the EWF image is a 2-step process:

  ✓ mount the EWF to be seen as RAW disk

  ✓ mount the raw disk

- Tools:

  ✓ Windows: `FTK Imager` (very simple)

  ✓ Linux has several options:

  - `ewfmount` or `xmount + mount` → requires `sudo`, but allows to see `MFT` as a file

  - `xmount + udisksctl` → the safest option, can be done by a regular user

Mount EWF image with `ewfmount` on Linux

1. `sudo ewfmount nps-2008-jean.E?? /mnt/raw`

   - maps as a RAW file

   - read only, it is not possible to emulate write operations

2. `sudo mount -t ntfs -o`

`ro,loop,show sys files,streams interface=windows,offset=$[63*512]`

`/mnt/raw/ewf1/mnt/loop/`

   - mounts file system in the RAW image

   - `show sys files` – allows to see NFTS structures as files

   - `streams interface=windows` – allows access to *Alternate Data Streams* (ADS) data

   - `offset=$[63*512]` – beginning of the partition to mount (in bytes)

Mount EWF with `xmount` on Linux (without `sudo`)

1. `xmount --in ewf nps-2008-jean.E?? --out raw --cache cachefile /mnt`

   - maps EWF as a RAW file

   - `xmount` emulates write operations using a cache file

2. `udisksctl loop-setup -f /mnt/nps-2008-jean.dd`

   - creates a loop device for each partition

   - `ls /dev/loop0*` → check how many partitions were identified

   - this command requires the user to belong to the `fuse` and `disk` groups:

     ✓ `sudo usermod -a -G fuse username`

     ✓ `sudo usermod -a -G disk username`

3. `udisksctl mount -b /dev/loop0p1`

   - mount the first partition

dcfldd

- developed by *Department of Defense Computer Forensics Lab* (DCFL)

- forensic tool derivate from the `dd` command line tool

- differences with `dd`

  - ✓ calculates the hash values and supports `md5, sha1, sha256` and `sha512`

  - ✓ can write the identified bad sectors to a separate file

  - ✓ can aggregate bad sectors errors `Had 1,023 'Input/ouput errors' between blocks 17-233'`

  - ✓ checks the hash values

  - ✓ reports the progress

  - ✓ allows to split the image file in smaller files

  - ✓ to ensure reproducibility bad sectors are written with zeros in the image file

- there are many forensic tools derivate from `dd`

  - ✓ `dc3dd` (very similar), `ddrescue, dd_rescue, rdd,...`

To get more info about the `dcfldd` tool

- `dcfldd --version` → installed version

- `dcfldd --help` → list all the supported options

- `man dcfldd` → man page

You can get more info:

https://dcfldd.sourceforge.net

https://forensics.wiki/dcfldd/

complement with info from https://en.wikipedia.org/wiki/Dd_(Unix)

dcfldd `if=/dev/sourcedrive hash=md5,sha256 hashwindow=1G md5log=md5.txt`

`sha256log=sha256.txt hashconv=after bs=512 conv=noerror,sync split=10G`

`splitformat=aa  of=image.dd`

- `if=/dev/sourcedrive` → file that represents the drive to acquire

- `hash=md5,sha256` → request `md5` and `sha256` hash values

- `hashwindow=1G` → calculate hash values at each `1 GB`

- `md5log=md5.txt sha256log=sha256.txt` → files name to store hash values

- **`hashconv=after`** → calculate hash values after error checking

- `bs=512` → use block size of 512 bytes

- **`conv=noerror,sync`** → `noerror` – doesn't stop in case of reading errors, `sync` – keeps image synced when errors show up

- `split=10G` → split RAW image into 10 GB files

- `of=image.dd` → base filename

- `splitformat=aa` → format of individual filenames `image.dd.aa, image.dd.ab,...`

```
cat SHA256.txt
```

0 - 1048576: 1756ad07245b68744644fa147bbed4dbf5b148ba61839d01e7421ff20098c681
1048576 - 2097152: 908348ee7e44372531d1311143d9ef3a2829fe30f93831b5a81e450a9d366168
2097152 - 3145728: 30e14955ebf1352266dc2ff8067e68104607e750abb9d3b36582b8af909fcb58
3145728 - 4194304: 30e14955ebf1352266dc2ff8067e68104607e750abb9d3b36582b8af909fcb58
4194304 - 5242880: 30e14955ebf1352266dc2ff8067e68104607e750abb9d3b36582b8af909fcb58
5242880 - 6291456: 30e14955ebf1352266dc2ff8067e68104607e750abb9d3b36582b8af909fcb58
…
52428800 - 53477376: 30e14955ebf1352266dc2ff8067e68104607e750abb9d3b36582b8af909fcb58
Total (sha256): 5767d9dcd2e48b3a0dce1b9a143ecf7a664364660637c5f348d1054afb4a1784

Guymager https://guymager.sourceforge.io

- very user friendly

- suppports `RAW`, `EWF` and `AFF` file formats

- faster than known commercial imagers running under Windows.

- does not support logical acquisitions:

  ✓ `/etc/guymager/guymager.cfg` – default configuration file, do not change!

  ✓ `/etc/guymager/local.cfg` – do all your configuration in this file, *e. g.* `EwfCompression=BEST`
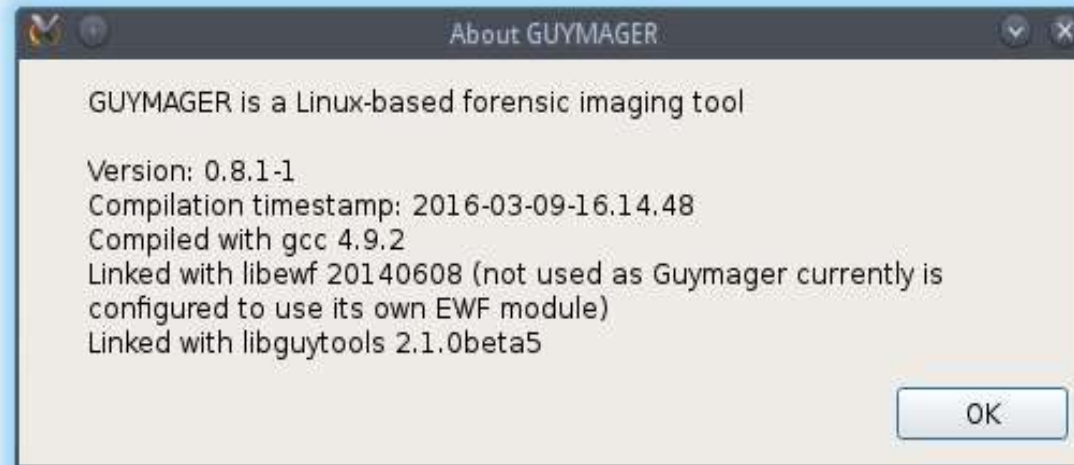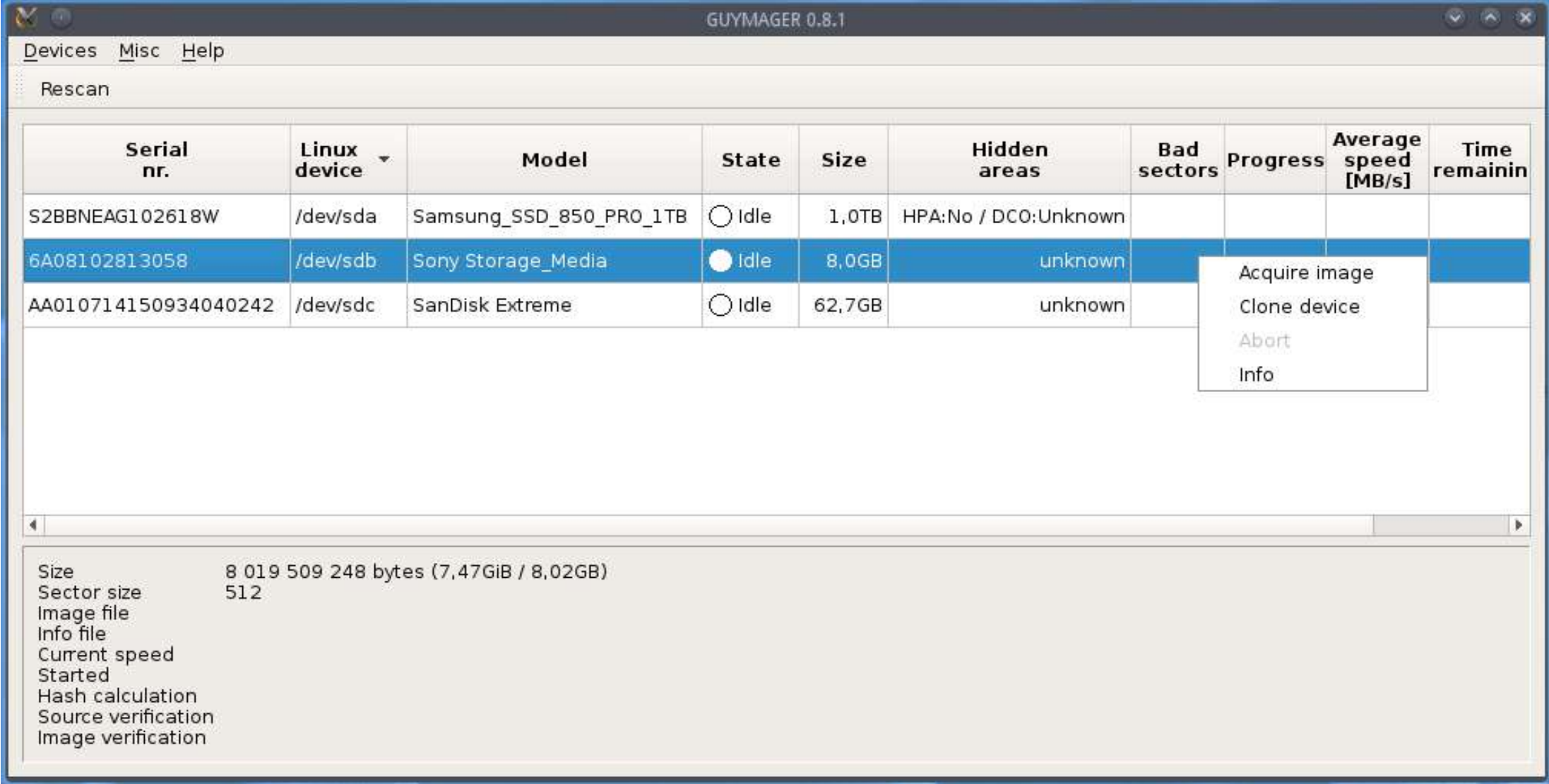
Recommended option for Linux

Paladin Toolbox https://sumuri.com/software/paladin

- included in the live Linux Paladin from Sumuri (forensics distro)

- free, but not open source and requires registration to download

- supports logical acquisitions, which is the recommend option for SSDs

Tableau Imager https://security.opentext.com/tableau/hardware/details/tx1
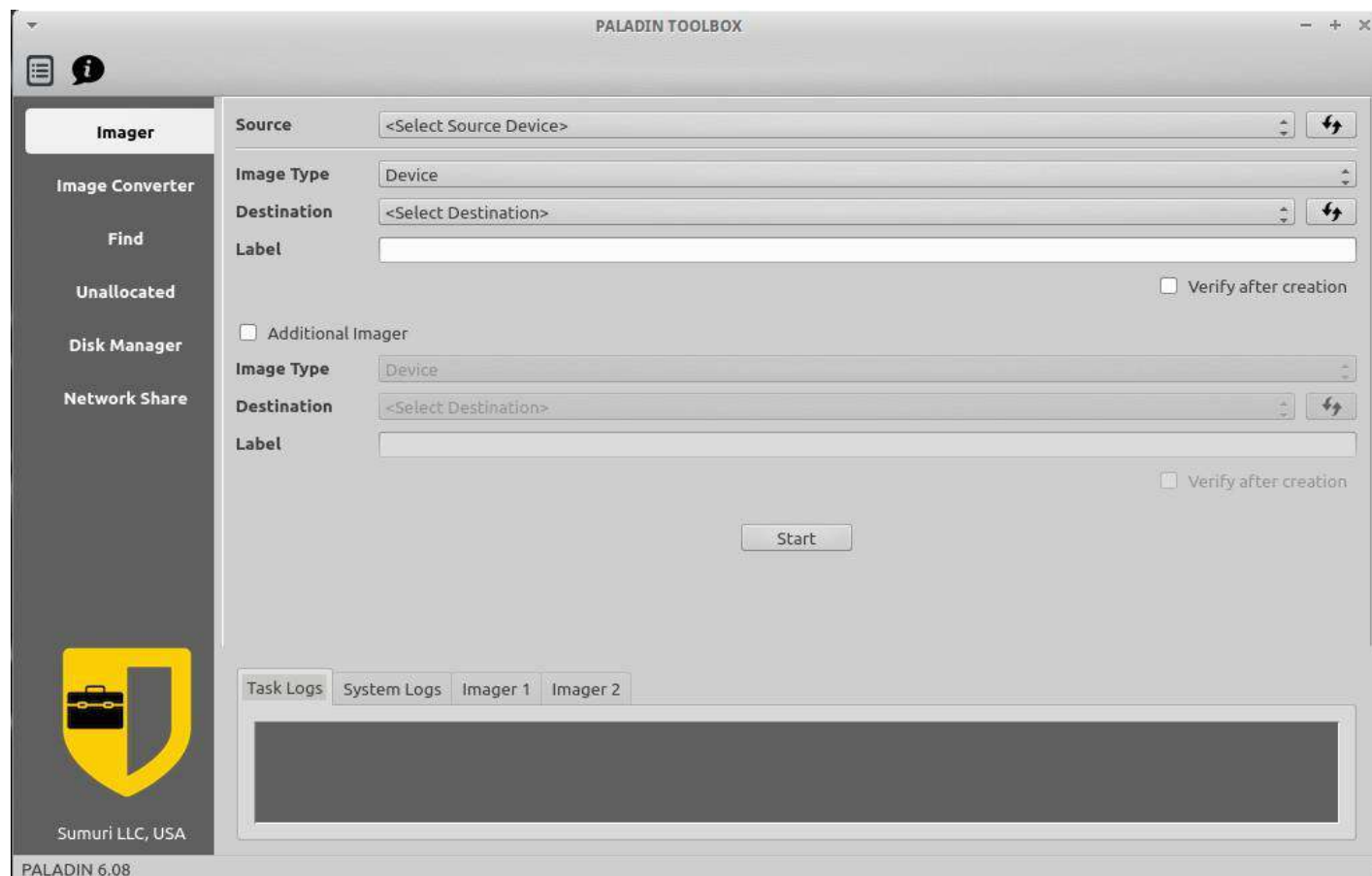
- works only with Tableau write blockers
- free, but not open source and requires registration to download
- does not support logical acquisitions, which is the recommend option for SSDs

FTK Imager https://accessdata.com/product-download/ftk-imager-version-4-5
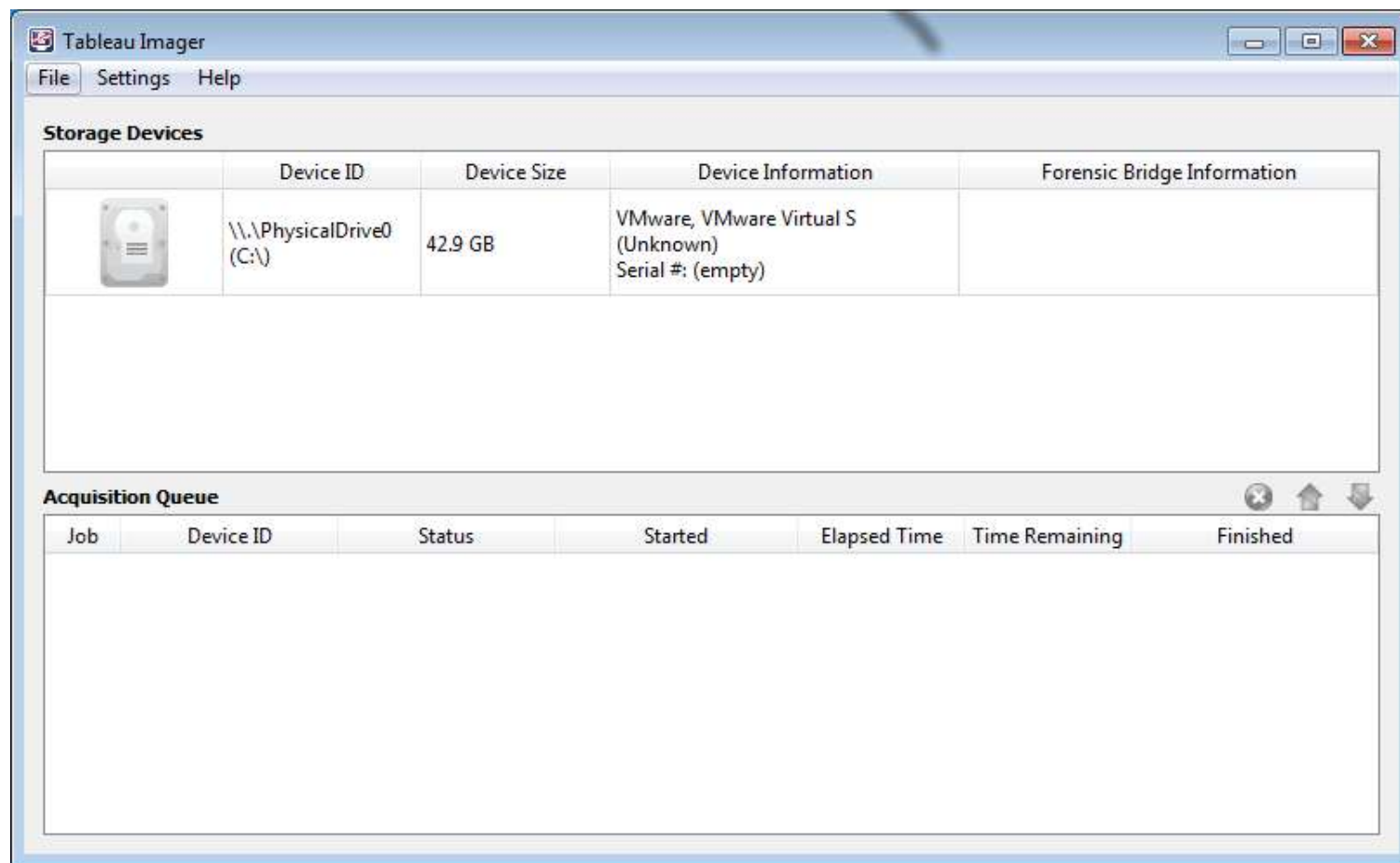
- Create forensic images of local hard drives, CDs and DVDs, thumb drives or other USB devices, entire folders, or individual files from various places within the media

- Preview files and folders

- Preview the contents of forensic images

- Mount an image for a read-only view

- Export files and folders from forensic images

- See and recover files that have been deleted from the Recycle Bin

- Create hashes to check the integrity of the files

- Generate hash reports for regular files and disk images

- Lite version runs as portable application

Recommended option for windows

- Lab 01 - Build WinFE and boot a virtual machine with it

- ## Lab 02 – Create a Forensic Image

1. Without extracting the virtual machine assigned to your team, add it as an evidence source to FTK Imager running on your computer

2. Create a .e01 forensic image from the virtual machine with FTK Imager
   - ✓ make sure you have enough disk space for the acquisition
   - ✓ split into 4 096 MB files to fit into FAT32 file systems if needed
   - ✓ enable compression, it's slower, but takes less space
   - ✓ validate the forensic image

- ## Lab 02 – Create a Forensic Image

3. Sign your forensic imaging acquisition report

As you already know, calculating acquired image hashes using summary functions is always good forensic practice. Don't forget that in addition to guaranteeing the **integrity** of the files, it is also convenient to guarantee their **authenticity** through a digital signature. I suggest you use Gpg4win (Windows) or GnuPG (Linux). They are easy to install and use:

Windows:
https://gpg4win.org/download.html (already contains Kleopatra frontend)

Ubuntu:
https://www.gnupg.org/download/index.html

Frontends:
sudo apt install gpa
sudo apt install kleopatra

Use hkp://keyserver.ubuntu.com server to export your public keys