Digital Forensics

Legal and technical aspects of digital forensics

Matej Kovačič
https://telefoncek.si

Digital Forensics in the Modern World: Problems of Theory and Practice

Tashkent, May 5th, 2023

Digital forensics

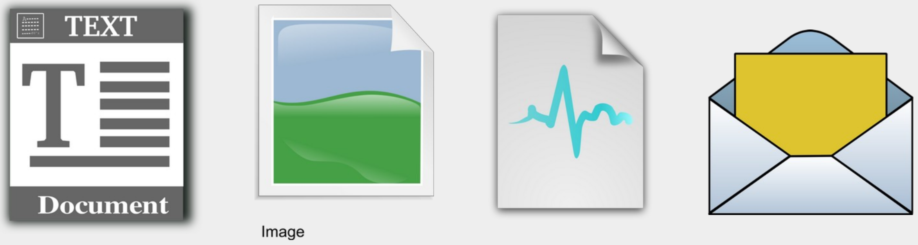
Digital forensics, also known as computer forensics, is the process of uncovering and analysing electronic data in order to gather evidence for legal proceedings.

It involves the use of various techniques and tools to examine digital devices such as computers, smartphones, and storage media to identify, preserve, analyse, and present digital evidence.

Digital evidence

Digital evidence refers to any data or information that is stored or transmitted in digital form and can be used as evidence in a legal investigation or trial.

Examples: e-mails, text messages, social media posts, digital images and videos, computer files, log files,...



Digital evidence

Digital evidence is often used in criminal investigations to help establish a suspect's **guilt or innocence**, and can also be used in civil litigation, regulatory investigations, and other legal proceedings.

The use of digital evidence has become increasingly important in recent years due to the widespread use of digital technologies and the amount of data that is generated and stored in digital form.

Information technology could be a target ("victim") of a crime, data carrier (evidence provider) or means for committing a crime.

Digital forensic principles

The forensic principles are a set of guidelines that govern the collection, preservation, analysis, and presentation of evidence in forensic investigations. These principles are designed to ensure that evidence is collected and handled in a manner that is **consistent with scientific standards** and that the evidence is **admissible in court**.

Forensic investigators must ensure that their findings are credible, reliable, and admissible in court. They do that by following **forensic principles**.

Digital forensic principles

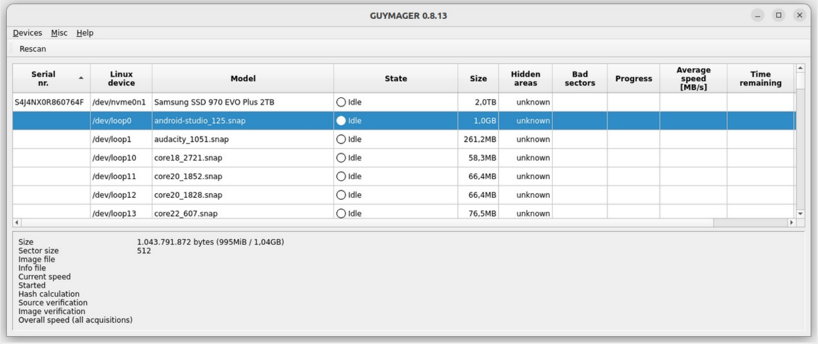
Documenting of all procedures

- All digital evidence forensic activities must be accurately documented, stored and accessible for review so that they can be repeated by an independent third party which should achieve the same results of the forensic analysis.
- ***Transparency***: The investigation process must be transparent, and all findings must be documented and communicated clearly.
- ***Reproducibility***: Forensic findings must be reproducible and verifiable by independent experts.
- ***Relevance***: Evidence must be relevant to the case and must be collected and analysed with a specific purpose in mind.

Digital forensic principles

Integrity of the data

- Evidence must be collected, preserved, and analysed in a manner that maintains its integrity and reliability.
- No process may alter the original copy of the data. Investigator must seize the data according to digital forensic principles and then perform a forensic examination of the data on a working copy of the original.
- Read only forensic copying.



Serial nr.	Linux device	Model	State	Size	Hidden areas	Bad sectors	Progress	Average speed [MB/s]	Time remaining
S4J4NX0R860764F	/dev/nvme0n1	Samsung SSD 970 EVO Plus 2TB	○ Idle	2,0TB	unknown				
	/dev/loop0	android-studio_125.snap	● Idle	1,0GB	unknown				
	/dev/loop1	audacity_1051.snap	○ Idle	261,2MB	unknown				
	/dev/loop10	core18_2721.snap	○ Idle	58,3MB	unknown				
	/dev/loop11	core20_1852.snap	○ Idle	66,4MB	unknown				
	/dev/loop12	core20_1828.snap	○ Idle	66,4MB	unknown				
	/dev/loop13	core22_607.snap	○ Idle	76,5MB	unknown				

```
Size                        1.043.791.872 bytes (995MiB / 1,04GB)
Sector size                 512
Image file
Info file
Current speed
Started
Hash calculation
Source verification
Image verification
Overall speed (all acquisitions)
```

Digital forensic principles

Objectivity and competence

- Collecting digital evidence requires specialized techniques and tools to ensure that the evidence is preserved and admissible in court. Digital forensic experts are often called upon to analyse and interpret digital evidence and to provide expert testimony in legal proceeding.
- Forensic investigators must remain *objective* and impartial throughout the investigation process.
- Forensic investigators must be *competent* and qualified to conduct their work, and they must adhere to accepted scientific standards.

Digital forensic principles

Data security

- ***Chain of Custody***: The chain of custody must be maintained for all evidence to ensure that it is not tampered with or contaminated.
- Chain of custody refers to the documentation and tracking of the physical custody of evidence from the time it is collected to the time it is presented in court. The chain of custody provides a complete record of the handling of the evidence (seizing, access, storage, transfer…), including who collected it, where it was collected, when it was collected, and who has had possession of it (and where) at each stage of the investigation (when, who, where, to whom and why).

Digital forensic principles

Data security

- The chain of custody is important because it helps to establish the authenticity, integrity, and reliability of the evidence. It ensures that the evidence has not been tampered with, altered, or contaminated in any way, and that it can be traced back to its original source.
- The chain of custody documentation must be accurate, complete, and maintained throughout the entire investigation process. Any gaps or inconsistencies in the chain of custody could raise questions about the validity and admissibility of the evidence in court.

Digital forensic principles

General forensic rules and legislation

- When working with digital evidence, general forensic rules and legal provisions for securing evidence must be taken into account.

Other important questions

- Who is the owner of the data?
- Where are the data located (physically), are the data accessible through the network?
- Data outside the country: territorial jurisdiction (court's power over events and persons within the bounds of a particular geographic territory) and subject-matter jurisdiction (the authority of a court to hear cases of a particular type or cases relating to a specific subject matter).
- The right to privacy (and also workplace privacy) and personal data protection legislation.
- Classified information handling.

Where is digital forensics used?

- **Criminal investigations**: Digital forensics is used by law enforcement agencies to investigate and prosecute a range of crimes, including cybercrime, fraud, corruption, theft, child exploitation, homicide, manslaughter, terrorism, etc.
- **Civil litigation**: Digital forensics can be used in civil lawsuits to gather evidence related to intellectual property theft, breach of contract, and other disputes.
- **Corporate investigations**: Digital forensics is used by companies to investigate employee misconduct, theft, fraud, and other violations of corporate policies.
- **Incident response**: Digital forensics is used in incident response to identify and contain security breaches and other cyber incidents.

Where is digital forensics used?

- **Compliance**: Digital forensics is used to ensure that organizations are complying with legal and regulatory requirements, such as data privacy and security laws.
- **Family law**: Digital forensics is sometimes used in family law cases to gather evidence related to child custody disputes or allegations of infidelity.
- The evidence collected during a digital forensics investigation can be used to support or refute a claim or allegation, and can help to identify perpetrators, exonerate innocent individuals, and provide valuable information for legal proceedings.

Typical digital forensic procedure

Identification: The first step in a digital forensics investigation is to identify the digital devices that may contain relevant evidence, such as computers, smartphones, servers, etc.

Chain of Custody: The chain of custody must be maintained for all evidence to ensure that it is not tampered with or contaminated. All procedures should be accurately documented.

Collection/seizure: Once the relevant devices have been identified, they should be secured and then forensic investigators will collect and preserve the digital evidence using specialized tools and techniques. This includes creating forensic copies of data to ensure that the original evidence is not altered or destroyed during the investigation.

Typical digital forensic procedure

Analysis: The next step is to analyse the digital evidence using specialized software and techniques to uncover relevant information. This may include examining file systems, analysing network traffic, or decoding encrypted data.

Reconstruction: Once the relevant information has been extracted from the digital evidence, forensic investigators will reconstruct the events that led up to the incident being investigated. This may involve piecing together fragments of deleted files, analysing communication records, or examining log files.

Presentation: Finally, the forensic findings are presented in a clear and concise report that can be used as evidence in court or in other legal proceedings.

Typical digital forensic procedure

Forensic investigators should communicate with their clients throughout the investigation process, but they must do so in a manner that is professional, transparent, and in accordance with ethical and legal standards.

Communication is essential to ensure that the investigation is conducted efficiently and effectively, and that the client is aware of the progress being made and any challenges that may arise.

However, it is important for forensic investigators to maintain objectivity and impartiality throughout the investigation, and to avoid any conflicts of interest that could compromise the integrity of the investigation.

Forensic acquisition

Forensic acquisition of data stored on:

- local data carriers;
- remote data carriers and data in the cloud;
- "live" device (with non-persistent data).

Forensic acquisition

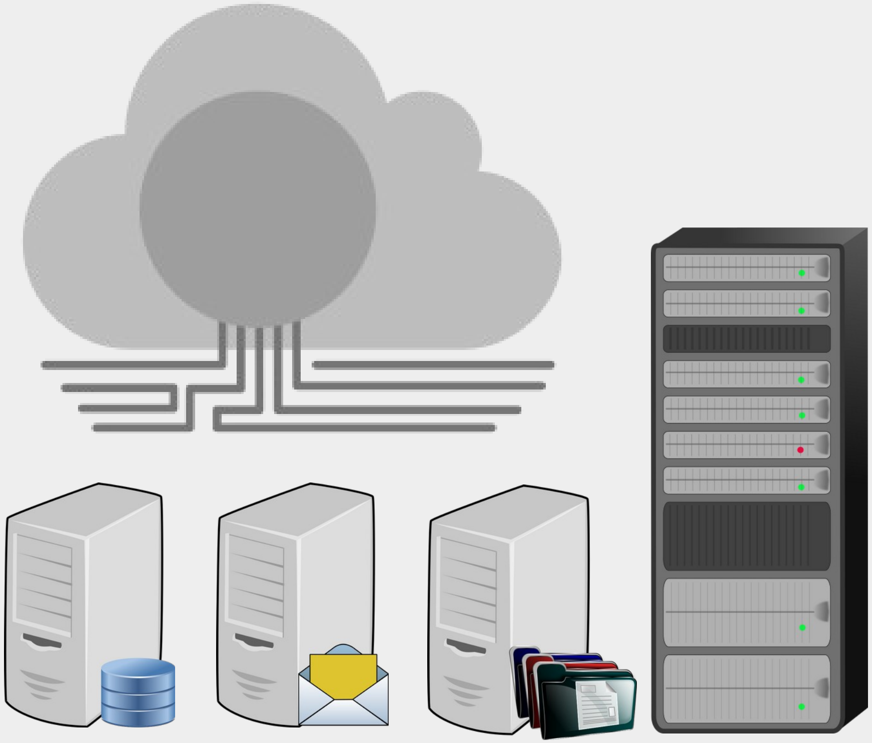
Local data carriers:

- Hard disks, SD cards,...
- SSD disks (and TRIM function and its impact on digital forensic examinations!)
- disk arrays: they are complex storage systems made up of multiple disks and controllers that work together. These systems can pose several challenges for digital forensic investigators, such as the distribution and striping of data across multiple disks.
- Other devices (cameras, printers, GPS, IoT,...).
- SIM cards.
- Mobile phones.
- ...

Forensic acquisition

Remote data carriers and data in the cloud:

- network data storage,
- databases,
- log files,
- mail, file and other servers,
- virtualisation,
- cloud storage,
- …



Forensic acquisition

Live forensic acquisition (with non-persistent data):

- ***Documentation***: Before starting a live forensic acquisition, it is important to document the state of the system and the procedures used to collect data to ensure the evidence is admissible in court.
- ***Identify volatile data***: Volatile data includes any data that is stored in memory, such as running processes, network connections, and system logs.
- Use the tool to collect the volatile data and save it to a forensically sound storage device.

Forensic acquisition

Special examples:

- Mouse jiggler: a device moving the computer mouse that prevents sleep mode or the screensaver from activating. Mouse jigglers are also known as mouse movers.
- Power override device: special UPS that enables transporting a live computer without shutting it down.

Forensic acquisition

Special examples:

- Faraday forensic analysis enclosures: they offer the RF shielding (radio frequency shielding) and hands-on accessibility for electronic device forensics investigations.

- Cold boot attack is a type of cyber attack that involves retrieving sensitive information, such as encryption keys or passwords, from a computer's RAM after it has been powered off or restarted. Normally, when a computer is powered off, the data stored in its RAM is lost. However, in a cold boot attack, an attacker can take advantage of the fact that RAM retains its data for a brief period of time after it loses power (a few seconds to a few minutes depending on the temperature).

Encryption (and possible solutions)

Encryption can pose significant difficulties to digital forensics, as it can prevent investigators from accessing or decrypting data on a seized device or to intercept or monitor data in transit, such as network traffic or data transmitted over the internet.

Encryption (and possible solutions)

Restoring backups

- Restoring data from backups (especially if they are not encrypted) can be helpful in cases where important data has been lost or deleted, as backups may contain valuable evidence that can be used to reconstruct the timeline of events or to identify key individuals or actions that led to the data loss.
- Backups could be stored in the cloud.
- Several backup solutions (especially the ones used in the cloud) are encrypting the data by default.

Encryption (and possible solutions)

Decryption

- The decryption process is nowadays usually not possible. Even if it is possible, it can be slow and resource-intensive, requiring significant computing power and time.
- Some encryption software or devices may include backdoors or other security flaws that can be exploited by attackers to bypass encryption, but nowadays this is usually not the case.
- Quantum resistant encryption algorithms.
- In some cases, a device may be encrypted with multiple layers of encryption, each requiring a separate decryption key or password.

Encryption (and possible solutions)

Decryption

- Plausible deniability refers to the ability of an encrypted container or file to appear to contain innocent or innocuous data, even if it actually contains sensitive or incriminating information. This is achieved through the use of hidden volumes or other techniques that allow the user to create multiple layers of encryption and present different passwords or keys to reveal different levels of data.
- Steganography is the practice of concealing a message or information within another non-secret message or object in such a way that it is difficult to detect or decipher. It is often used in conjunction with encryption to provide an additional layer of security and to prevent the detection of the encrypted data.

Encryption (and possible solutions)

Decryption

- Hiding information within image files, audio files, or other types of media.
- There are tools and techniques available to digital forensics investigators to detect and analyse steganographic data, but they are not 100% reliable.
- In some cases, it may be possible to compel a criminal suspect to provide their password or encryption key through legal means, such as a court order or search warrant. Since this is inherently coercive and may be ethically problematic.

Encryption (and possible solutions)

Decryption

However:

- This must be authorized by law and must not violate the suspect's constitutional rights.
- Even if a suspect is compelled to provide their password or key, there is no guarantee that this would be effective. There are several encryption systems that are designed in a way that makes it impossible for the suspect to reveal the password or decryption key, even if they are compelled to do so. These systems rely on advanced cryptographic techniques such as *One-Time Pad* (OTP), *Perfect Forward Secrecy* (PFS), *secure enclave/hardware security module*, *homomorphic encryption*, etc.

Encryption (and possible solutions)

Live forensic acquisition (with non-persistent data)

- Live forensic acquisition could be a solution, however there might be in place technologies to detect and/or block live forensic acquisition.

Evil Maid attack

- An Evil Maid Attack is a type of cyber attack in which an attacker gains physical access to a target computer or device in order to install malware or steal sensitive data.

Encryption (and possible solutions)

Evil Maid attack

- The attack typically involves the attacker gaining access to the target device when the owner is not present, such as when the device is left unattended in a hotel room. The attacker then uses various techniques to gain access to the device, and to steal sensitive information or plant malware to steal encryption keys/passwords.
- There are several countermeasures against Evil Maid attacks (for instance secure boot, two-factor authentication, tampering detection, etc.).

Encryption (and possible solutions)

Source wiretapping (lawful interception at the source)

- Source wiretapping, also known as lawful interception at the source, is a technique used by law enforcement or intelligence agencies to intercept communications at the source, before they are encrypted or otherwise secured.
- The purpose of source wiretapping is to enable law enforcement or intelligence agencies to intercept and monitor communications between individuals who may be engaged in criminal or terrorist activity.

Encryption (and possible solutions)

Source wiretapping (lawful interception at the source)

- Source wiretapping is typically carried out under the authority of a court order or other legal process, but it is a controversial practice, because it can be abused to violate the privacy rights of innocent individuals or to conduct mass surveillance without adequate oversight or accountability.
- Usually it is done with special software tools (malware, trojan, spyware), which could be installed on the target device and can wiretap at the source (before data are encrypted).

Cyberweapons

»This spyware tool is designed to secretly turn mobile phones - both with Android and iOS operating systems - into 24-hour surveillance devices, as it grants complete and unrestricted **access to all sensors and information of the targeted device**. It can read, send or receive messages that should be end-to-end encrypted, download stored photos, collect passwords, hear and record voice or video calls as, among other things, it has full access to the phone’s camera, microphone, and geolocation module.«

Pegasus and surveillance spyware. Report for European Parliament,
May 2022.

Encryption (and possible solutions)

Source wiretapping (lawful interception at the source)

- Today the market for such tools is well developed and there are several spyware cyberweapons available (for instance FinFisher, Pegasus, Predator, Black Cube, Blue Hawk CI, BellTroX, Cytrox107, Predator, Candiru, Subzero/KNOTWEED, etc.).
- There are technical countermeasures to detect or even block the use of these tools on mobile phones and computers.

Encryption (and possible solutions)

Traffic data and meta data analysis

- Traffic data analysis can help investigators to detect who is communicating with whom and when. Typical examples are call logs.
- Metadata analysis is the process of examining metadata associated with digital files to gain insights into the origin, context, and history of the files. Metadata is essentially "data about data" and can include information such as the creation date and time, author, file size, location, and other relevant details.

Encryption (and possible solutions)

Traffic data and meta data analysis

- Data retention is controversial because it violates the right to privacy of innocent people and can lead to mass surveillance. In some countries, courts have ruled that data retention laws are unconstitutional or otherwise illegal.
- There are technical measures to prevent traffic data analysis (for example using anonymisation networks) and technical measures to automatically remove metadata from files.

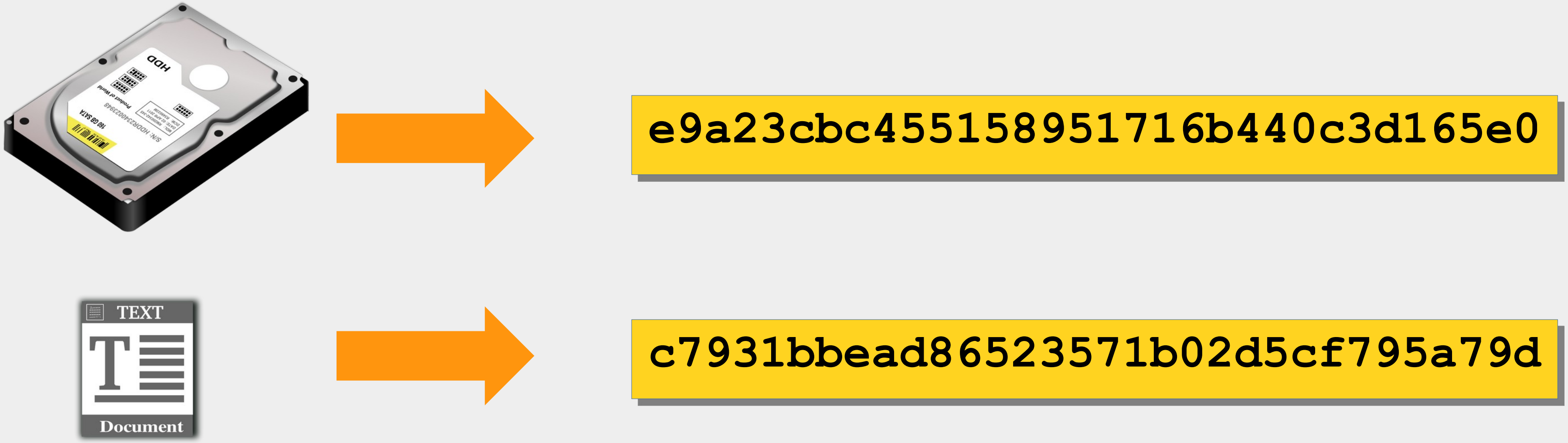
Encryption (and possible solutions)

Network traffic forensics

- Network forensic analysis can be used in criminal investigations to gather evidence, especially traffic data.
- Investigators can identify communication patterns and trace the origin and destination of messages.
- With use of machine learning and AI technologies, investigators can identify suspicious patterns of activity or communications.

Hash algorithms

Cryptographic hash functions are mathematical algorithms that are used to map data of arbitrary size to a fixed-size output. The resulting hash value is unique to the input data and is typically used to verify the integrity and authenticity of the data.



e9a23cbc455158951716b440c3d165e0

c7931bbead86523571b02d5cf795a79d

Hash algorithms

One-way mathematical function, collision-resistant and avalanche effect.

Examples:

MD5:

75222cee3990e39e9fb48fa7ca6a733b

SHA-1:

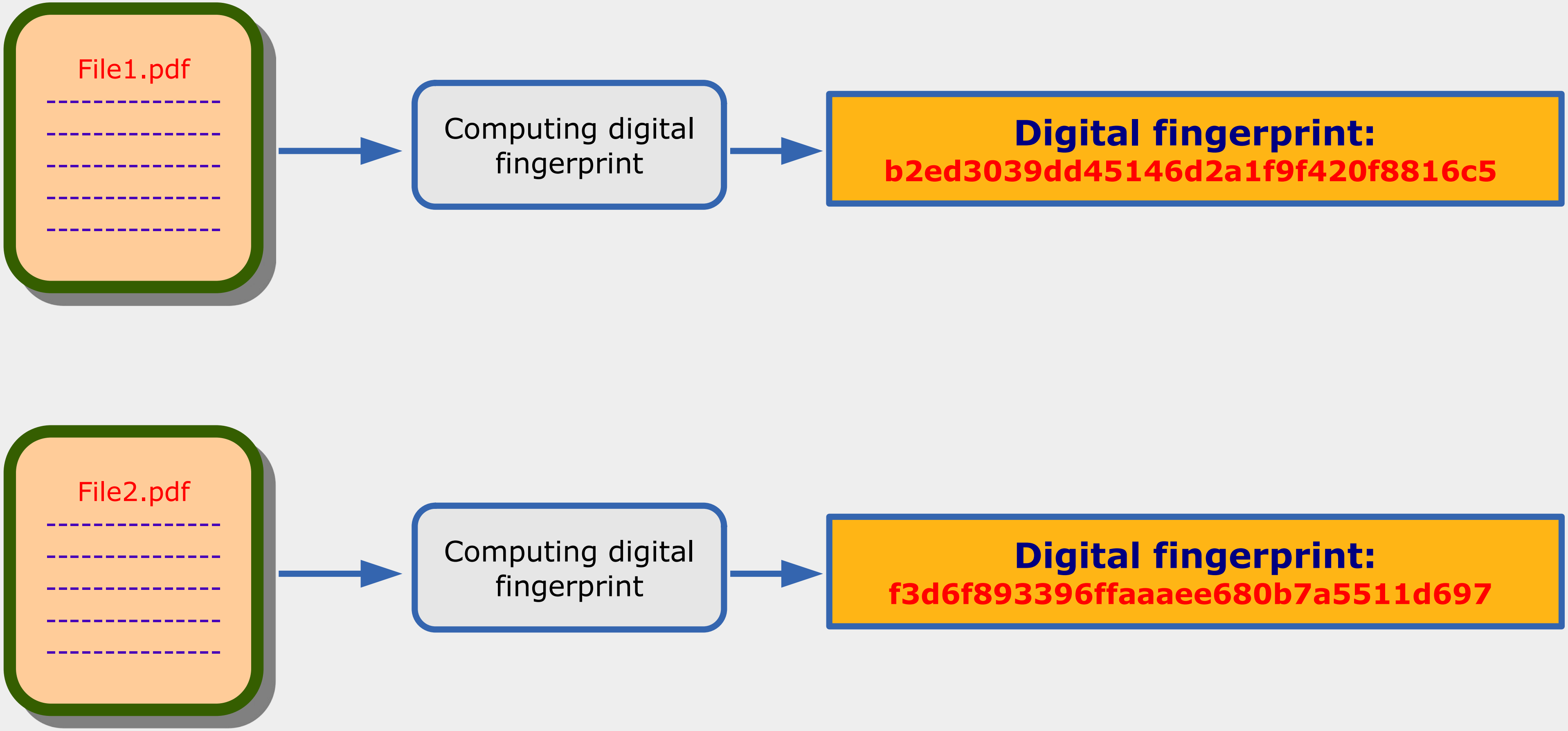
1f149834675ab2ae6d076ee3cbaa9158b6864ee1

SHA-256:

3226338fb2c35ca40d39de77a0735779b1c0886f39a3762de2b502901567d39e

Hash algorithms

Use: file identification (known good files, known bad files).



File1.pdf

Computing digital fingerprint

Digital fingerprint:
b2ed3039dd45146d2a1f9f420f8816c5

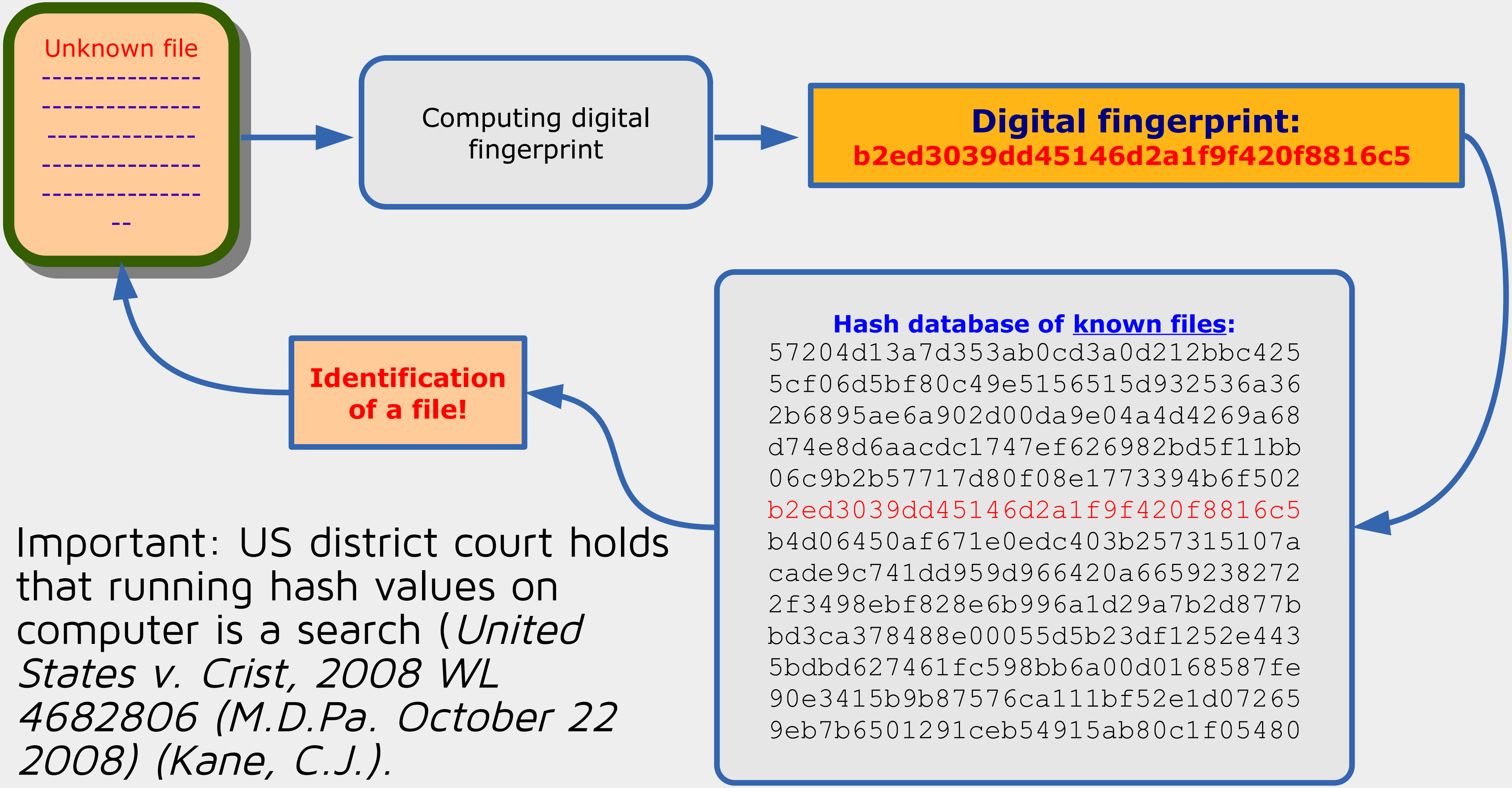
File2.pdf

Computing digital fingerprint

Digital fingerprint:
f3d6f893396ffaaaee680b7a5511d697

Hash algorithms

Use: file identification (known good files, known bad files).



Unknown file

Computing digital fingerprint

Digital fingerprint:
b2ed3039dd45146d2a1f9f420f8816c5

Hash database of known files:

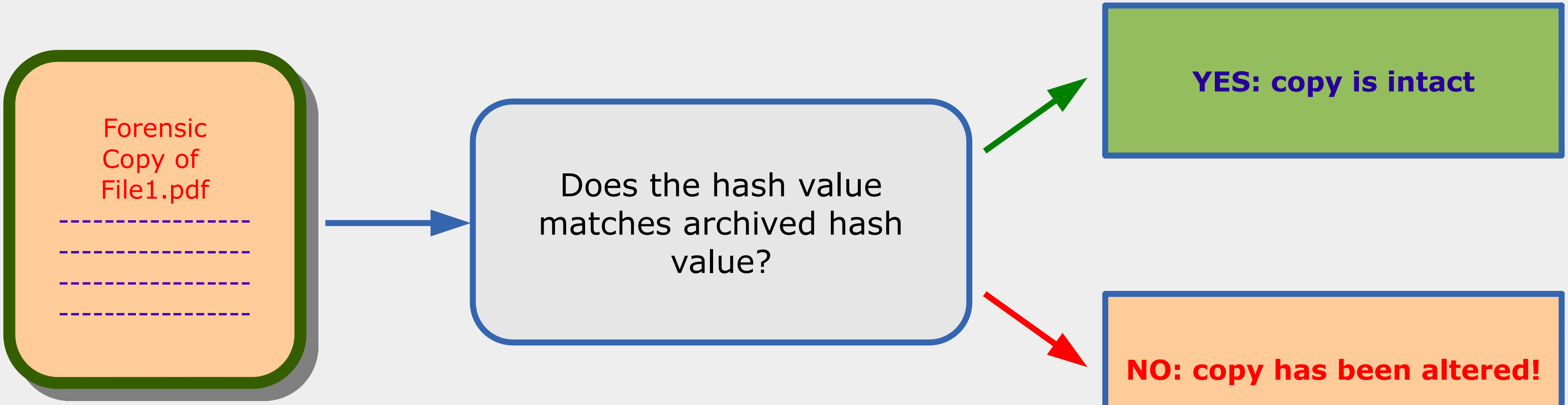
```
57204d13a7d353ab0cd3a0d212bbc425
5cf06d5bf80c49e5156515d932536a36
2b6895ae6a902d00da9e04a4d4269a68
d74e8d6aacdc1747ef626982bd5f11bb
06c9b2b57717d80f08e1773394b6f502
b2ed3039dd45146d2a1f9f420f8816c5
b4d06450af671e0edc403b257315107a
cade9c741dd959d966420a6659238272
2f3498ebf828e6b996a1d29a7b2d877b
bd3ca378488e00055d5b23df1252e443
5bdbd627461fc598bb6a00d0168587fe
90e3415b9b87576ca111bf52e1d07265
9eb7b6501291ceb54915ab80c1f05480
```

Identification of a file!

Important: US district court holds that running hash values on computer is a search (*United States v. Crist, 2008 WL 4682806 (M.D.Pa. October 22 2008) (Kane, C.J.).*

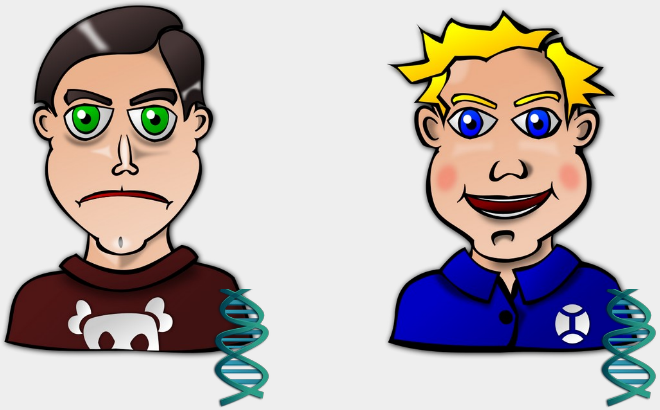
Hash algorithms

Use: ensuring data integrity (in digital forensics).



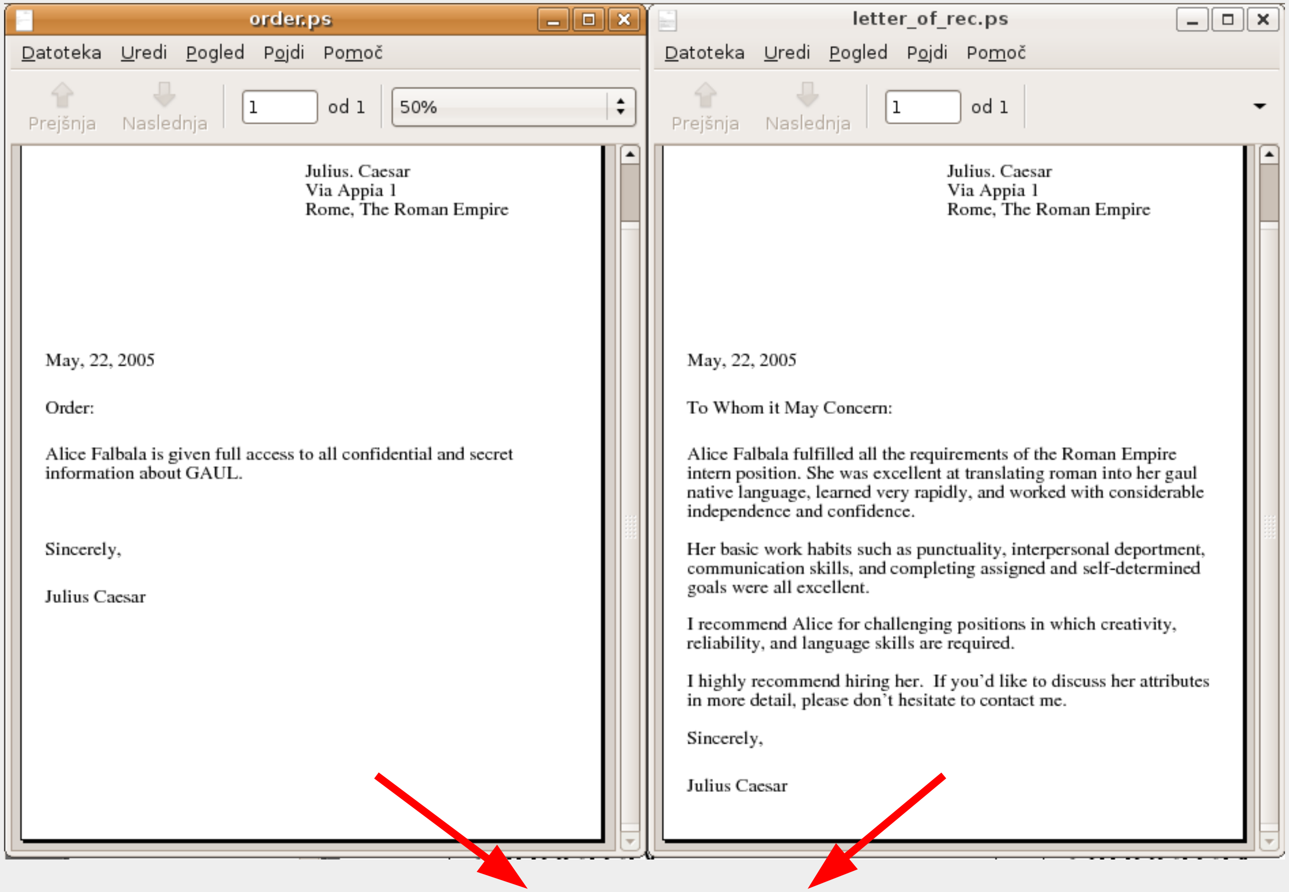
Hash algorithms

A collision occurs when two different sets of data produce the same cryptographic hash value. Collision can compromise the integrity of the data because it means that two different sets of data have produced the same result, making it impossible to determine which set of data is the original one (incitement of evidence or destruction of evidence).



It is the same situation as we would have two totally different persons with the same DNK!

Hash algorithms



Julius. Caesar
Via Appia 1
Rome, The Roman Empire

May, 22, 2005

Order:

Alice Falbala is given full access to all confidential and secret information about GAUL.

Sincerely,

Julius Caesar

Julius. Caesar
Via Appia 1
Rome, The Roman Empire

May, 22, 2005

To Whom it May Concern:

Alice Falbala fulfilled all the requirements of the Roman Empire intern position. She was excellent at translating roman into her gaul native language, learned very rapidly, and worked with considerable independence and confidence.

Her basic work habits such as punctuality, interpersonal deportment, communication skills, and completing assigned and self-determined goals were all excellent.

I recommend Alice for challenging positions in which creativity, reliability, and language skills are required.

I highly recommend hiring her. If you'd like to discuss her attributes in more detail, please don't hesitate to contact me.

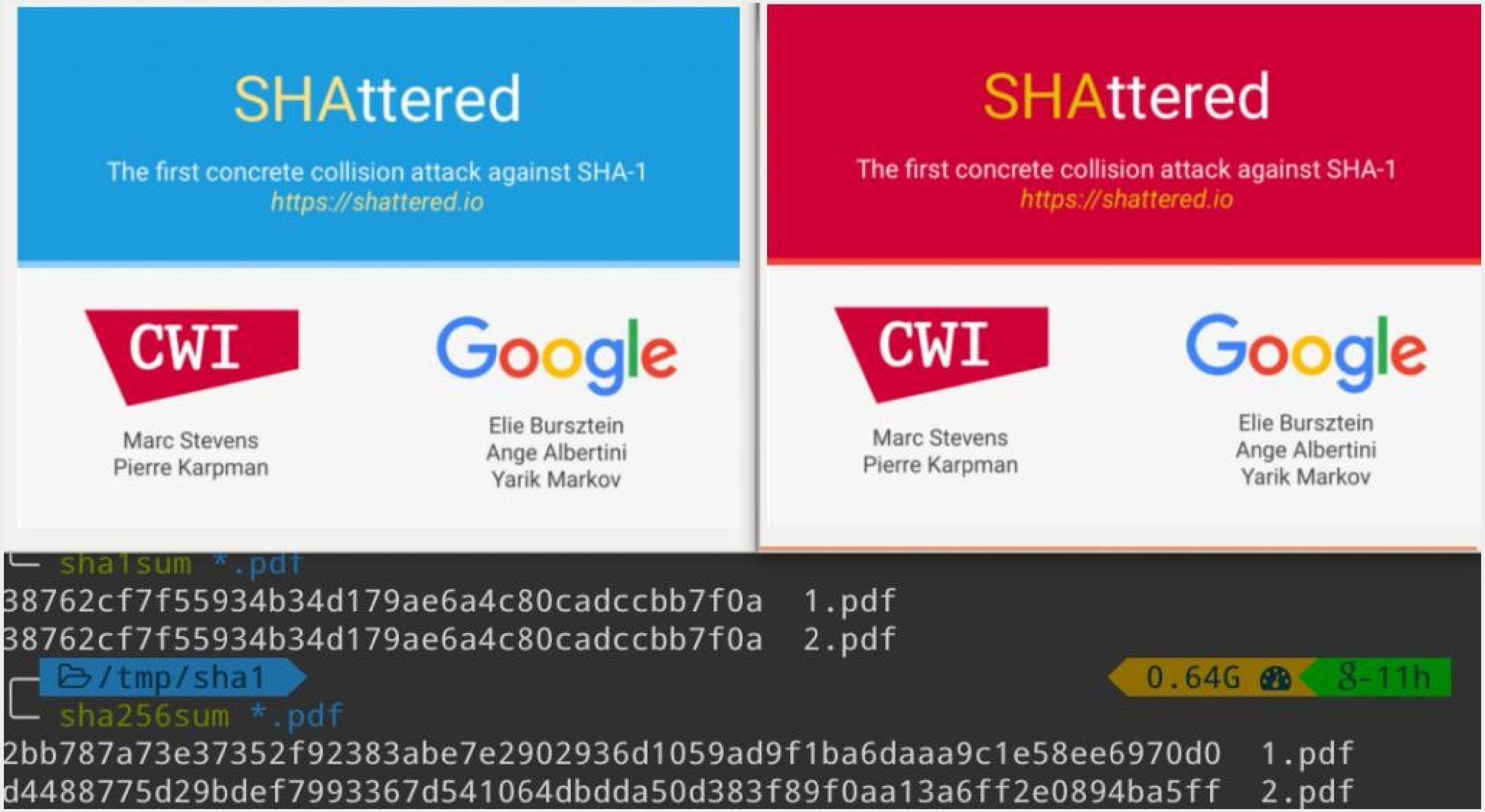
Sincerely,

Julius Caesar

MD5: 5421a523481fdc6a2a1c832e72c7b8a5

Source: Magnus Daum and Stefan Lucks. 2005. The Story of Alice and her Boss: Hash Functions and the Blind Passenger Attack. Eurocrypt 2005.

Hash algorithms



SHAttered

The first concrete collision attack against SHA-1
https://shattered.io

CWI

Marc Stevens
Pierre Karpman

Google

Elie Bursztein
Ange Albertini
Yarik Markov

SHAttered

The first concrete collision attack against SHA-1
https://shattered.io

CWI

Marc Stevens
Pierre Karpman

Google

Elie Bursztein
Ange Albertini
Yarik Markov

```
└─ sha1sum *.pdf
38762cf7f55934b34d179ae6a4c80cadccbb7f0a  1.pdf
38762cf7f55934b34d179ae6a4c80cadccbb7f0a  2.pdf
┌─ /tmp/sha1                                                    0.64G   8-11h
└─ sha256sum *.pdf
2bb787a73e37352f92383abe7e2902936d1059ad9f1ba6daaa9c1e58ee6970d0  1.pdf
d4488775d29bdef7993367d541064dbdda50d383f89f0aa13a6ff2e0894ba5ff  2.pdf
```

SHA-1: 38762cf7f55934b34d179ae6a4c80cadccbb7f0a

Source: Marc Stevens, Elie Bursztein, Pierre Karpman, Ange Albertini and Yarik Markov. 2017. The first collision for full SHA-1. <https://shattered.io/>

Questions?

Matej Kovačič

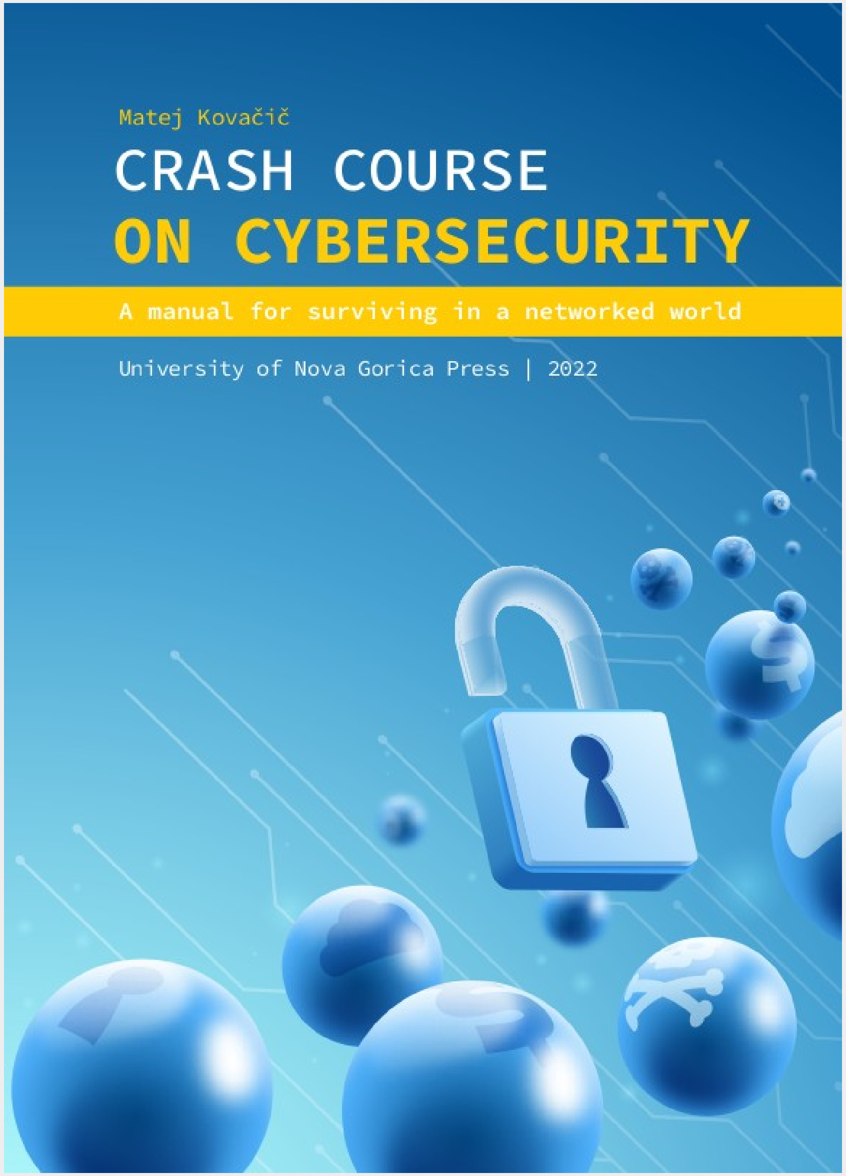
https://telefoncek.si

Some further reading...

Matej Kovačič. 2022. Crash course on cybersecurity: a manual for surviving in a networked world. ISBN: 978-961-7025-24-8 (PDF)

The book tries to explain the complex area of cybersecurity in an understandable way, to help to grasp the essential information on how to protect yourself and/or your company from cyberattacks and to provide technologically neutral advice for the implementation of protection against cyberattacks.

The book is available under a Creative Commons license and PDF is freely available online.


Matej Kovačič
CRASH COURSE
ON CYBERSECURITY
A manual for surviving in a networked world
University of Nova Gorica Press | 2022