Introduction to Digital Forensics

Nicola Fröhlich, Amir Hosh
Lecture Script

Examiner: Prof. Dr. rer.nat. Frank Kargl
Supervisor: Dominik Lang

Submission Date: March 7, 2019

Issued: March 7, 2019

Contents

1 Introduction

1.1 Organisation

Please see lecture slides.

1.2 Educational Goal

The educational goal of this lecture is to raise the students' awareness of problems and challenges of digital forensics. In this lecture, the topic of digital forensics will be introduced and special topics of digital forensics will be considered. At the end of the lecture the students should understand that evidence traces in systems can be changed or destroyed very quickly. Students should also understand that digital forensics is not only important in law enforcement but also particularly in IT security and that even IT security experts have to understand not to behave like an bull in a china shop after an incident.

1.3 Motivation

Over time, more and more technologies have been developed and extended. Society has developed technologies to help and support people. This development found its way into every area of life. In companies every step is often recorded and managed digitally. The organisation and production are already fully automatised. In daily life the new technologies have increased their impact. Nowadays every person has a smartphone or a smart wearable. Even in our homes, there are smart household appliances and corporations are no exception. We are always accompanied by an electric device.

These technologies should support and help people, but they also help people with less noble intentions. Everywhere in the world, there is criminality. **Criminality** never sleeps and is as old as humanity. Unfortunately technologies do not only simplify things in daily life but also crimes. Crimes with technical support, so called **cybercrimes** or **computer crimes**, increase and cause estimated damage of tens of millions of euros every year. This amount is only estimated because many incidents are not reported and experts estimate the dark figure of the not reported incidents

to 90%. Enterprises do not report an incident because they are scared of damage to their reputation.

To counteract the increasing cybercrime, law enforcement agencies, as well as the companies, are preparing themselves in order to handle incidents. Digital forensics is used to investigate crimes in law enforcement as well as in companies to solve incidents in order to improve their own cyber defence or to seize digital evidence traces of a possible crime and to be aware not to destroy them. [28][30][44]

1.4 Definition

In general **digital forensics** handles traces of uncleared incidents. These traces are seized in order to understand the actions of the incident and to reveal their real nature.

One kind of handled incidents are crimes. Crimes which are committed by or aim at digital systems are often called cybercrimes or computer crimes. In literature there is no uniform definition of the words cybercrime and computer crime.

The *Cambridge Dictionary* defines the word **cybercrime** as an *"illegal activity that is done using the Internet"* [13]. The German Duden, however, defines the word cybercrime as "illegal acts in the computer and telecommunications sector, especially over the Internet" [19]. But with this definition, all computer-related crimes are cybercrimes not only the ones which use the Internet.

In other sources like the *Bundeslagebild Cybercrime 2017* of the German *Federal Criminal Police Office* (Bundeskriminalamt, BKA) cybercrime is divided into cybercrime in the narrower sense (crimes committed against data networks, information technology systems or their data) and in the broader sense (crimes are committed by means of information technology) [11].

The different versions of the *Convention of Cybercrime* also have a mixture of terms in use. In the German version the term "Computerkriminalität" (literally translated "computer criminality") and in the English version "cybercrime" is used [14].

Interpol divides Internet-related crimes into "advanced cybercrime" (attack against computer hardware and software) and "cyber-enabled crimes" (for example, crimes against children) [37].

So you see, a completely clear definition is complicated. We will assume the definition of the Cambridge Dictionary and a definition of the Bavarian Police for computer crime.

Computer crime

"Computer crime is understood as the committing of criminal offences using computer systems" (Bavarian police) [5]

Cybercrime

"Illegal activity that is done using the Internet"
(Cambridge Dictionary) [13]

1.5 Area of Application

The application of digital forensics takes place in the fields of law enforcement and IT security. Sometimes the application of digital forensics is not directly named as digital forensics especially in the area of IT security.

1.5.1 IT Security

In the application area of corporations digital forensics takes place when an incident appears. If an incident occurs in a corporation, the question which has to be answered is if it is really not just a business disruption. But directly after an incident this is not clear. So the IT experts should behave as if the system got attacked by an offender because only then they will not destroy evidence traces for a possible later complaint.

Here, an *Incident Response Team* should be established and trained in the company. Such a team has to be practised in the use of IT security as well as digital forensic tools and techniques. Without adhering to the principles of digital forensics, IT security experts may be not capable of solving and learning from the attack because from destroyed traces cannot be learned. Even IT security experts need the evidence traces in the system in order to understand the occurred attack and to improve the defence of the system based on the used mechanisms and exploits. [10][28]

1.5.2 Law Enforcement

In the criminal prosecution evidence of crimes is examined in order to determine the innocence or culpability of a defendant and to reconstruct the actions. In these investigations evidence is collected and there is much digital evidence these days. Nearly every committed crime has digital material to provide because everywhere we go, we carry a digital device with us or there are digital devices around.

The first responders on a crime scene or the police officers of a lawful search have to be up to date with the new development with pieces of evidence as well because without the trained police officers at the scene digital evidence would be overlooked. [2]

The application of digital forensic examiners in the area of law enforcement is diverse in Germany. The State Offices of Criminal Investigations of the different federal states are searching and hiring digital forensic experts and there are external service providers for the digital forensic examination as well.

Digital forensic examiners are not cyber criminal investigators with police training. Forensic examiners are scientists. At the police, police officers can be forensic examiners, but they do not have to be and the other way round. Digital forensic examiners work for criminal investigators and answer their questions in the lab. Digital forensic examiners are authorised experts and can perform in court.

There are external service providers for digital forensics. These companies can be contacted when a judge or a crown prosecutor needs new answers to some questions as well as when a company has the suspicion that an employee is doing something illegal. The external service provider will make an expert assessment and this can serve as a valid evidence in court. [2][56]

1.6 Outlook

In the following lecture the area of digital forensics will be examined and for this it is unimportant if digital forensics is applied in law enforcement or in the IT security area because just the documentation and presentation of the results could be different then. The lecture has only an introductory character to the topic and does not cover every detail of digital forensics.

In general the lecture will cover the topics of digital forensics and concerned laws on a local and international basis in general. Then more technical topics as computer, mobile, and network forensics are approached. Additionally anti-forensics is discussed which provides some ideas of the used techniques of criminals to prevent digital forensics.

2 Digital Forensics

When a crime occurs, the police have to investigate the circumstances of the crime. In a murder, for example, the coroner and the forensics come in order to document exactly any traces found. Witnesses are interviewed and maybe possible suspects interrogated. The police collect any information about the event of the crime to reconstruct it. For the reconstruction, forensic science is used to evaluate the traces found at the crime scene.

2.1 Forensic Science

In the past, crimes were solved with the help of testimonies and extorted confessions. But since the 19th century and the early 20th century forensic science has been used for law enforcement. Since then the usage of forensic science has been developed over hundred years to get established in court. Over the years the usage of forensic science has started to be standard to solve crimes and incidents. Forensic science was developed and had time to establish standards and principles. Today forensics is an indispensable part of combating crime and civil cases. Scientifically substantiated DNA analyses and ballistic standards have been developed that are currently established in the criminal investigation for solving, for example, a gang shooting and are accepted in court. All procedures of the modern forensic science are meant to be scientifically sound and proven. [2]

One of the reasons why science is used to solve crimes could be the conviction of a French criminologist. At the beginning of the 20th century Edmond Locard framed one of the forensic science principles, the **Locard's Exchange Principle**. [50]

Locard's Exchange Principle

There is an exchange of traces between objects when they get into contact.

But nowadays, crimes are committed by means of digital devices or at least they accompany the perpetrator or incidents arise in IT systems. Here the *Locard's Exchange Principle* is not directly applicable to digital information because digital evidence does not react like physical evidence. Digital evidence has other characteristics than usual physical evidence, such as volatility and changeability. Therefore, as computer criminality increases, digital evidence had to be accepted at a court of law. So

experts had to develop standards and principles to apply forensic science to digital information to guarantee a reliability of digital evidence and to meet the requirements of evidence for the court. Digital forensics was born.

At the first Digital Forensics Research Workshop (DFRWS) in 2001 digital forensics was defined. [2]

Digital Forensics

Digital Forensics is the scientific use of methods on digital evidence to reconstruct unauthorised actions.

Nowadays every investigation of a crime contains the examination of classical forensic evidence as well as the analysis and evaluation of digital data. The evidence of an incident at a company often is only digital. So the digital part of an investigation is a systematic examination of seized data by scientific methods. The systematic examination of a crime serves to reconstruct the actions of the crime.

With the examination, the identification of key facts about the incident is done and then they will be answered. For a murder, for example, the answers to the questions who is the murderer and why the offender did it are particularly important for the judge in court. But there are more objectives of an investigation which have to be met. These **objectives** of an investigation depend on the investigation itself and the present situation. An investigation in a jurisdictional matter will aim at different objectives than a corporate one. The main questions about an incident are: "what happened, where did it happen, when did it happen and how did it happen?". Other more difficult questions are: "why did it happen and who did it?". The question about the who is often the most difficult one. In a corporate investigation about an incident, the question about what could be learned from the incident is also an important matter to improve the own cyber defence. [10][28][2]

Objectives of an Investigation

What, Where, When, Why, Who, How, Lessons learned

2.2 Digital Evidence

When it comes to the examination of an incident, the team of the crime scene investigation or the *Incident Response Team* of a company restrains evidence at the scene like fingerprints, DNA traces or digital devices connected to the incident. Forensically collected digital data is called digital evidence and is the basis of digital forensics.

Digital Evidence

Digital evidence is defined as any digital data independent of its form which contains probative information about an incident.

But this digital evidence is sometimes hard to find. Some storage media are as small as a fingernail and can hold several gigabytes of data or the evidence data is stored on an unknown faraway server. These situations often occur with SD cards and surveillance cameras. Likewise, evidence data may be hidden among other large amounts of data.

So in an examination of digital evidence, a forensic analyst has to structure, evaluate and identify the digital evidence in a scientific way. In short, the examiner sheds light on the enormous amount of collected data. With this procedure, the analyst gathers information about the incident.

With digital evidence, the analyst has to distinguish between traces left by the people and traces left by the computer. The two different kinds of traces are referred to as **digital archaeology** and **digital geology**. *Digital archaeology* comprises the traces which are left by the machine operator, so human behaviour produced the traces. On the other hand, *digital geology* are the traces which are produced by the computer system itself. Investigations often target information about the system operator, but for that, the analyst has to understand the behaviour of the system itself. [2][56]

2.2.1 Principles

For a valid theory about the incident, the examiner has to be sure to have no corrupted evidence and safety mechanisms have to be used to control it.

Example

At an indemnity of a surveillance system, for example, timestamps are changed during the securing procedure. The examiners have to know that they have corrupted evidence because then they can consider the corrupted timestamps in their analysis.

To process the resulting traces of a system correctly, procedures have to be developed for the practitioners. In digital forensics, there are principles which guarantee that the investigation is accomplished correctly and the evidence preservation is handled perfectly. These will ensure the acceptance of the evidence in court.

In order to fulfil these conditions, the investigation has to be forensically sound. That means that the used procedures correspond to the scientific method which means

that the processing of digital evidence is a systematic and reproducible examination and evaluation of hypotheses of the incident. Ideally, the scientific method should be established in every forensic standard and principle. [2]

Forensic Soundness

An investigation is sound if the used procedures are approved by digital forensic principles, standards and processes.

With the **forensic soundness** of an investigation, the procedures on digital evidence are reproducible and understandable by a third party with the same tools and source material.

Example

Assuming that the first analyst finds an encrypted folder at a specific path, breaks the encryption and finds child pornographic files in the folder, each of the steps of the examination has to be documented exactly. So that a second analyst can understand and repeat these steps and will come to the same conclusion.

So, one of the principles of digital forensics is the **evidence integrity** because of the characteristics of digital evidence, digital evidence is easily changed. [2]

Evidence Integrity

Evidence integrity is the preservation of the original traces without any changes, be it also by accident.

This principle is an ideal because often the collection of the evidence requires a change of the evidence. When an analyst acquires digital evidence from a running system or a network, the evidence data will be changed. So, the analyst has to document every step which the examination takes exactly to consider the changes in the analysis later.

The intentional change of evidence by a person will be prevented by the use of the **double-verification principle**. So one person controls the other and the other way round. And besides, nobody can pin misbehaviour on the analyst because there is a witness. [2]

Double-Verification Principle

Verification and control by two parties.

Another principle of digital forensics is called **chain of custody**. The chain of custody describes the documentation of the exact steps of an investigation. The documentation is made so that it is documented when and who did which steps in the examination of the evidence and how the digital evidence was processed. [2][56]

Chain of Custody

Documentation of every step during the examination of the evidence.

Now the principles of digital forensics are known and in the following section the general procedure of an investigation of an incident is described and explained. In practice, these steps are often not clearly marked out in each investigation.

2.3 Digital Forensic Process

So far, we have discussed the terminology of digital forensics and the speciality of digital evidence, and the fact that the examination of an incident has to follow scientific methods.

Over the years a digital forensics process has been developed to ensure that the forensic investigation is forensically sound, as defined above, and the forensic principles are deployed. This process is universal and can be applied in every context such as a criminal, corporate or even a private investigation.

2.3.1 Requirements

There are requirements for the forensic process, or rather for the methods and tools used to assure that the investigation is sound and also court-enforceable. The requirements for the forensic process are *acceptance, reliability, repeatability, integrity, cause and effect, and documentation.* Some of these requirements are also covered in the forensic principles. [28]

The requirement of **acceptance** means that the used methods and tools should be accepted in the scientific world. If methods which are not established are used, however, a proof of correctness has to be given. So it is possible to use other techniques than the established ones, but then you have to prove the correctness of your investigation and to argue for your choice.

Reliability means that the used tools are resilient and the functionality of the method or tool is comprehensible.

The **repeatability and reproducibility** of each step in an investigation is an important requirement to ensure that the evaluation of the evidence is not corrupted. So, a third party can verify the result of an investigation by repeating the investigation steps and come to the same conclusion.

The **evidence integrity**, which has already been mentioned before, is one of the requirements of an investigation. In every investigation, the integrity of the evidence has to be secured and proven. Otherwise, an evidence could be manipulated and second-guessed in court.

The requirement of **cause and effect** claims that with the investigation methods reasonable links can be established. The events that happened should be meaningfully connected with the evidence found and the persons involved.

The **documentation** of the examination is a really important matter in a forensically sound investigation because a good documentation of each step in an investigation meets all the requirements and makes it comprehensible to foreigners. A saying in digital forensics is that when something is not documented, it did not happen [56]. [10][28]

Negative Example

In a blackmail case, for example, an offender blackmails the victim by email. These emails are manually secured on an external storage medium. During the backup the documentation is flawed. The backup of some emails is documented, some others are secured, but not documented. The forensic analyst starts the examination of the emails and finds hints to the blackmailer in the attachments to the emails with a special metadata tool. To top it all, the analyst forgets to produce hash values over the original data and his examination copy. The analyst writes his report and the case comes to court a few months later.
In this case, the analyst appears as an expert witness in court and has to present his results. During his statement, questions arise like where the analyst got this additional email which is not listed in the documentation, how he found the hint exactly and whether the analysed emails are the same as the original ones which were secured from the offender's computer. The analyst will find it difficult to answer any questions and proof the answers in his testimony.
Thus, in the worst case, the court gets the impression that the emails might have been tampered with and slipped, and the evidence is declared invalid.
Here, the problem is that the requirements for an investigation were not met. The documentation of the backup of all emails was not consistently enforced, neither a proof of the integrity of the evidence, nor a description to reproduce the steps of the investigation were given.

It is therefore very important to fulfil the requirements in an investigation so that

you have a proof of what has been done with the evidence and that the investigation is understandable by non experts like the court.

The summarised requirements are listed below:

- **Acceptance** - The used procedures should be generally recognised among experts or the proof of correctness of the procedure must be provided.
- **Reliability** - The functionality of the procedure should be scientifically proven.
- **Repeatability** - A third person has to come to the same result using the same procedure and the same source material.
- **Integrity** - The digital evidence must not be changed intentionally or by accident.
- **Cause and Effect** - By the procedure, links between evidence traces of events and persons should be established and logically comprehensible.
- **Documentation** - Every step in the procedure has to be documented exactly.

When all the requirements are fulfilled, the investigation should be sound and usable in court. [10][28]

2.3.2 Forensic Process

The forensic process itself can be divided into two main phases, before the incident and after the incident. The exact sections of the process are chosen differently in each source, but all of them describe the same approach. So in this lecture, we will divide the whole process into seven sections which are used **iteratively** if necessary for the investigation. For your information, in some sources the preparation before the incident is divided into the operational and the strategic preparation or it is just called **digital forensic readiness**. [10][28][2]

- **Forensic Readiness** - The strategic and operational preparation happens before any incident has occurred. This phase contains the organisation in the corporation or an agency to handle an incident. Here the authorisation and jurisdiction are clarified. The data protection should be clarified with the privacy officer and the authorisation should be obtained from the management to handle an incident immediately. An emergency guide and protocols should be developed and an incident response team should be established. The incident response team should practise the usage of forensic tools and should decide and organise which tools they want to use. This part of the forensic process in some sources is divided into the *strategic* and the *operational preparation* before an incident.

- **Identification** - In the first phase after the incident, the possible digital evidence is identified. Here, the scene of the incident, like the structure of the system, is documented and the affected devices by the incident of the system are determined and thus the digital evidence is also identified.

- **Collection** - The collection phase refers to the acquirement of the digital data from the identified devices. From every evidence device, a forensic duplication is made. This means the evidence data is copied. It is also called imaging and the forensic duplication is called an image. The images are secured with cryptographic hash functions to ensure the integrity of the evidence.

- **Examination** - In the examination phase, the collected data gets prepared for the analysis. Here the encrypted data is decrypted if possible, compressed data gets extracted and deleted data gets carved out of the unallocated space. The data just gets restructured so that during the analysis the data does not have to be processed anymore. This part of the process is time-consuming because the computers need calculating time.

- **Analysis** - In the analysis phase, the analyst searches for clues for or against a hypothesis or to answer the questions of a court. To find these clues matching with hash value databases, keyword searches or pattern matching and timelining are used, for example.

- **Documentation** - In this phase, the final report is made. In the final report every step and decision in the investigation are described and listed. The results are outlined and every information about the case which was collected or learned is mentioned. The final report is the result of the investigation.

- **Presentation** - For every ordering party, a final report has to be made and often presented in front of the management or a court of law. In a criminal investigation, an expert assessment is made and the expert has to testify in court.

This is the forensic process in general. This process is not always applicable to every incident, but it is better to have a guideline. [10][28][2]

Concrete models for the forensic process are the **S-A-P model** and the **Investigative Process Model**. The *S-A-P Model* divides the process into three big phases called “Secure”, “Analyse” and “Present” and the *Investigative Process Model* divides the process into 12 different phases. [4][10]

So, as you see, every model has different stages in the process, but the approach is the same.

2.4 Acquisition of Evidence

Before the processing of digital evidence can be started, the digital evidence has to be identified and collected. The identification of the evidence devices is part of the phase *Identification* of the forensic process and the collection of evidence happens in the phase *Collection* of the process.

2.4.1 Aquisition

The collection of digital evidence is also called **acquisition**. The acquisition secures the digital evidence data on other storage devices. These external storage devices have to be professionally wiped. The **wiping** is necessary to prevent to have old traces of data on the storage device. So it has to be sure that every single bit on the storage is overwritten before the external storage is used for an acquisition of evidence. [2]

The acquisition of data should always create the fewest changes to the system's data as already mentioned in the principle of *evidence integrity* in the section Principles of section 2.2 Digital Evidence.

There are two different kinds of acquisition of digital evidence, the post-mortem analysis and the live forensics. These two types differ in the way how the backup is done and the time of the analysis of the data. [10]

- **Post-mortem Analysis** - The post-mortem analysis is the examination of the digital data of a switched off system. The hard drives are removed and an image is made. The analysis of the evidence data happens afterwards. The collected data is persistent.
- **Live Forensics** - In live forensics, the analyst starts with an already running system. The acquisition of the evidence happens during run-time. This kind of acquisition will change the system itself like files and date stamps, so every step has to be documented quite well with time designation. With live forensics volatile data can be collected.

The first steps with digital evidence devices are quite important in order to make the right decision on the kind of acquisition. Therefore, the first person at the scene of an investigation has to make important decisions. The forensic analyst has to ponder different facts.

2.4.2 Order of Volatility

An important role in a digital crime scene acquisition plays the **order of volatility** of the data. The order of volatility denotes the acquisition chronology by the durability of the data as soon as power is lost. The most volatile data, for example, is lost after

nanoseconds and to this data belongs data in the system registers and in the RAM. The most persistent data have a storage time of years to decades. Persistent data is stored on CD-ROMs, DVDs and SSDs. [2][56]

Order of Volatility [2, p.31]

Type of storage	**Time lifespan**
System registers, peripheral memory, and caches	Nanoseconds
RAM	Ten nanoseconds
Network state	Milliseconds
Running system processes	Seconds
Data on disk (Cache)	Minutes
Cloud storage	Months to years
HDD data storage	Years
Floppies and other magnetic tape-based media	Years to decades
CD-ROMs, DVDs, print-outs	Decades
Read-only memory, flash and SSD data storage	Decades to centuries

2.4.3 Acquisition Steps

The first step in an acquisition is to clarify the **power status** of the evidence device in a digital crime scene to identify which kind of volatile data is available.

If the device is *switched off*, the device is photographed, documented and unplugged. Digital evidence devices are carried in *Faraday bags* to prevent the wiping of the device by remote access. For the acquisition, the hard drives are removed and the data is acquired. The decision about the volatility of the data is not necessary because at a switched off system there is only persistent data.

If the device is *turned on*, the decisions are more complicated. The forensic analyst has to decide between turning the device off or doing a live forensic analysis. Both approaches have their advantages and disadvantages.

By *turning off* the system, a perpetrator can be withhold to do any more damages, but volatile data about the incident will also get lost.

With a *running system*, the volatile data will be preserved, but the system will be changed. But decrypted data of an encrypted hard drive can be accessed and some malware are only available in the RAM, for example. A perpetrator could be observed and the attack analysed.

If the decision was not to turn off the system, then the **network status** has to be considered.

If the incident is long over, the data about the network status should be collected and the network should be turned off in order to prevent an external wiping of the

system, for example. Every step in the acquisition has to be documented exactly. Then a live forensic analysis can be done.

But if the perpetrator is still in the system, an expert has to decide to let the incident go on to observe the perpetrator and analyse him or to bounce him out of the system by turning off the network connection.

In order to make these decisions, a quick risk analysis should be done by the persons in authority. [10][2]

2.4.4 Imaging

To complete the acquisition of the digital evidence, the data of identified relevant devices has to be secured. This process is called **imaging** and it is an important part of an investigation because it ensures that the evidence can be used in court. If this process is applied incorrectly, the following analysis is useless.

Imaging

Imaging is the process in which a forensic duplication of evidence is created.

If the system is not running, the hard drives are removed from the system for the imaging. Then the data is copied with a **write blocker** to an external storage device, so a secure forensically sound copy is made of the evidence. Write blockers can be software or hardware based and the function of them is just to prevent any change of the evidence data. The image is a forensic duplication of the original evidence and will be used to do copies for the analysis. [10][2]

An analyst always works only on a copy of the secured digital evidence in order to prevent any changes to the original or to make it possible to go back to an unchanged status of the digital evidence if problems arise during the examination. Should it be necessary to investigate an original proof directly, then the analyst must be very experienced and careful. Moreover, a very good reason for this decision must be given because this could reduce the credibility of the evidence in court.

The image of the evidence can be a physical or a logical one. The **physical forensic copy** is a **bit-by-bit copy** of the storage and also contains the unallocated space. The **logical** one only copies the logical structure and its data, and does not capture the unallocated space. The physical image is the first one an analyst will try to produce, but for some devices, like, for example, smartphones and tablets, it is sometimes not possible to create a physical copy. Then, a logical copy is made. [2][56]

During the imaging process, the acquisition software is always running on an external drive and the forensic duplication is copied to a separate media. The acquisition of mobile devices proceeds in a different way. But this topic is handled in Chapter 6 *Mobile Forensics*.

2.4.5 Storage Formats

After the imaging process, the storage of secured digital evidence data is a challenging matter because the evidence has to be stored in a consistent way according to the above approached principles. To fulfil the requirements, different storage and exchange formats have been developed. There are a lot of different commercial and open source formats. The forensic storage formats differ in their capabilities and not every forensic tool can handle each format. Nearly every developer of forensic tools has his own format. So, in the following section, some evidence formats and their file extensions are listed:

- Raw Image Format (.dd)
- EnCase Evidence File (.E01)[32]
- Logical Evidence File (.L01)[32]
- Custom Content Image (.AD1)
- Advanced Forensic Format (.AFF)

2.4.6 Hashing

During the creation of the storage format of digital evidence many formats calculate **hash values** of the individual files and the entire evidence file to ensure the required evidence integrity. To ensure the evidence integrity, after every process of copying or each step of the examination, the produced hash value of the original image file and the actual one can be compared.

These hash values also help to reduce the workload of an analyst and to simplify the analysis. For this, the hash values of the individual files of the image are compared with different databases of operating system providers, law enforcement agencies and anti-virus software manufacturers. These databases save hash values of original system files or of pictures which have already been identified as paedophiliacs. So the analyst does not have to evaluate these files anymore and the big amount of data is reduced. [2]

Example

In a child pornographic case, for example, the analyst gets the data of all the digital devices of the suspect. These devices contain over a hundred thousands of individual files, but the law enforcement only wants to get the answer to a specific question. So the analyst has to go through all the files to identify the relevant files. With the hash values he can eliminate already as child pornographic identified pictures and videos, and only has to classify the reduced remaining ones.

Thus, all the specialities of the acquisition of digital devices are mentioned. So you see, the non forensic experts, too, have to have basic knowledge of digital forensics in order not to destroy the evidence as a first responder. [10][2][56]

2.5 Specialised Fields

The topic of digital forensics is a very broad one and it is still evolving. Digital forensics has many different specialised fields because it has to follow every new technological development. In literature, many special fields are named and defined differently. So do not be surprised about similar names for the same areas or a finer granular subdivision of an area.

The most common fields sorted by device are:

- Computer Forensics
- Network Forensics
- Internet Forensics
- Cloud Forensics
- Mobile Forensics
- Car Forensics

Specialised fields sorted by file formats are:

- Multimedia Forensics
- Image Forensics
- Audio / Video Forensics

Other specialised forensic fields:

- Memory Forensics
- Malware Forensics
- Anti Forensics

So, the work as a forensic analyst, has always something new and something old. That's why the work of a forensic analyst is so challenging and interesting. With every new invention a new field of digital forensics arises and this will not change because every piece of data is possibly usable for an investigation of a crime.

During the lecture we will take a closer look at the areas of computer forensics, network forensics and mobile forensics. Other areas covered include multimedia forensics and anti-forensics.

2.6 Further Reading

For a good overview over the topic digital forensics in the context of law enforcement the study of the book [2] is recommended. For the enterprising area the guideline [10] of the German Federal Office for Information Security could be read. The book [28] is a combination of both and looks furthermore at forensic tools.

In order to deepen different digital forensic process models the articles "The Enhanced Digital Investigation Process Model" [4] and "An Examination of Digital Forensic Models" [54] are recommended. For more information about digital evidence storage formats the article "Storage and exchange formats for digital evidence" [24] of a Norwegian University (today called Norwegian University of Science and Technology, NTNU) is useful.

2.7 Summary

In this chapter the definition by the Digital Forensics Research Workshop in 2001 of digital forensics was given to clarify the field of digital forensics. For an investigation of a crime the objectives are important milestones on the way to clarifying the entire crime. To find the answers to the objectives, digital evidence has to be examined. Digital evidence must be treated differently from the classic evidence, as digital evidence is very vulnerable to intentional or unintended changes. In order to prevent any changes, principles have been developed like the chain of custody, evidence integrity or double-verification principle. To examine and analyse the digital evidence, it has to be collected first. This is called acquisition. There are two types of acquisition and analysis, post-mortem and live forensics. The first is deployed at a powered off system, the other at a running system.

During the acquisition a forensic duplication of the evidence data is created and gets hashed with cryptographic hash functions to ensure the evidence integrity. A digital

forensic process was developed and requirements to the investigation process were formulated to make sure that the principles are observed. The process can be divided into the preparation before an incident and the phases after the incident occurred. The preparation before an incident is also called the digital forensic readiness and encompasses the strategic as well as the operational preparation. After the incident occurred, there are 6 different stages of investigation. The stages are the identification, the collection, the examination, the analysis, the documentation and the presentation at the end of an investigation in front of the management or in court.

2.8 Review Questions

1. What is the Locard's Exchange Principle and what does it mean?
2. What do you understand under the term "Digital Forensics"?
3. Which questions are answered during an investigation and how are the questions also called?
4. Which principles are important regarding digital evidence?
5. Which requirements should be met for the forensic process?
6. Describe the digital forensic process.
7. Which types of a forensic analysis exist and what are their differences?
8. What is the order of volatility?
9. Which facts should be considered in an acquisition?
10. What is imaging and which are the different types?

3 Digital Crime - Law and Consequences

This chapter is about the relevant laws concerning computer criminality and how important it is for a forensic analyst to have a basic understanding of the legal aspects of the discipline.

In the first chapter *Introduction* the definitions of the terms "cybercrime" and "computer criminality" were given and clarified.

In this chapter, you will find a synopsis of the laws on an easy level and the laws selected are only a summary of the relatively complex legal situation. The liability for any inaccuracies cannot be accepted. If you need legal assistance, please ask your lawyer. The relatively complex legal situation is a combination of data protection rights and criminal law.

The regulation of computer criminality and cybercrime is provided by different laws on an international and national level. On the international level, there are the *General Data Protection Regulation (EU-DSGVO)* [21] of the European Union as well as the *Convention on Cybercrime* [14], or also called the Budapest Convention, of the Council of Europe. On the national level, computer criminality is regulated among others in the *German Criminal Code (Strafgesetzbuch, StGB)* [69] and the *German Copyright Act (Urheberrechtsgesetz, UrhG)* [29], for example. [28][34][2]

3.1 Legal System

In general, the law is a complicated construct of different rules and regulations. One of the most important criminal laws is the first paragraph of the *German Criminal Code*. This paragraph states that an act without a prior law that classifies this act as a crime is not a crime. This circumstance is also substantiated by *Art. 103 Abs. 2* of the *German Basic Law (Grundgesetz, GG)* [31]. [60]

> §1 Keine Strafe ohne Gesetz, StGB

This means that any offence that could be committed with computers must be covered by a law to enable criminal prosecution. Because of this circumstance, a race to catch up in law was created with the development of technology in order to cover

the accrued dangers. With computer systems, new crimes become possible and computer systems also give a new dimension to conventional crimes. Now burglary can happen physically as well as digitally and digital devices can accompany traditional crimes and can serve as evidence.

Several crimes would not be unlawful with the jurisdiction of the last century. In the case of child pornographic writings, some sort of works were not unlawful before the year 2015. Posing writings are illustrations of children in special sexual seeming positions. These writings were not chargeable before 2015.

Digital data can serve as evidence but digital evidence is vulnerable to change and manipulation. For this reason, the conditions for a forensic examination mentioned in Chapter 2 must be met in order to increase the permissibility. If there is any doubt about the credibility of the evidence in court, the probative value can drop to zero. Thus, the traceability of the integrity and authenticity of the data must be given in the documentation in order to prevent it. [34]

Digital data are usually brought to court by an **appraiser** or expert who presents and evaluates the expert assessment or report. In court, the appraiser is interviewed as an **expert witness** and included in the state of evidence. So the probative value also depends on the credibility of the expert witness. The expert witness only vests significance to the material proof. In the German legal system, the exact handling of an expert report also differs in the law of criminal procedure from civil procedure law in relation to the admission as evidence. [34][70][78]

The expert witnesses are supposed to present **only facts and figures**. They must not include their own opinion in their speech in court. The professional evaluation of the evidence found must be clear and distinct from the facts. If the referee puts his own opinion in the report, his credibility could be questioned and thus all the evidence. The entire personality could be questioned and that is why it is not easy to be an expert in court.

An expert witness may be a person from a special police department or an external reviewer from a digital forensics service provider. Companies often have their own incident response teams and so their own forensic experts, or they engage an external team of experts to help with the clarification of incidents. [28][34][2]

3.2 Problems of Computer Criminality

The fight against computer and cybercrime faces many problems. The problems of combating computer crimes spring from the characteristics of the crime. The characteristics of digital crimes are different from the characteristics of common crimes.

The most significant characteristic of cybercrime is that the involved IT systems are often widely **distributed** over areas.

The computer of the victim is, for example, located in Germany but the perpetrator sits in front of his computer in America. The national jurisdiction of the victim can

start to investigate but they have only authority on their territory.

The authority of a jurisdiction is **limited to its nation state**. Additionally, it is possible that a lot of digital devices are involved in the crime and it is hard to identify them.

So, the jurisdiction of the victim needs assistance of other nations to solve the crime or at least to identify all the involved devices and systems as evidence. Different crime scenes have to be examined at a similar level to guarantee the reliability of the evidence in court.

But in diverse nations, there are different laws in force. In some states, an offence is declared as a crime by law and in others, the same act is not. So **safe havens** exist for criminals and not every request for assistance will be answered. To solve these problems, different nations have to agree on one common ground.

At last another problem is **time**. If the offence is illegal in all involved nations and the nations have decided to work together, the problem of collecting the evidence in time is still exist. Digital data has the nature to be overwritten over time and to be deleted, so it can vanish. Therefore the investigators and the bureaucracy have to be fast to be able to collect the relevant evidence in time. Additionally, in different nations, there are different rules for evidence and about what is allowed to get the needed evidence. Thus the cooperation for solving the crime in time is also a matter of the similarity of the jurisdictions. The time problem is aggravated by the existing time difference between the nations.

To counter these big problems in the fight against computer criminality, international treaties as the Cybercrime Convention are being signed between nations. [2]

At first, we will talk about the international treaties to combat computer criminality and then we will draw parallels in the German jurisdiction.

3.3 Convention on Cybercrime

The **Convention on Cybercrime** is an international treaty about computer criminality concluded by the *Council of Europe (CoE)* [14]. The treaty was submitted for signature in November 2001 and entered into force in July 2004. Germany signed the treaty 2001 and ratified it in 2009. [16]

The Cybercrime Convention is an international treaty and the nations which have signed have to implement the treaty in their national law. Four nations only signed the treaty and 61 nations have already ratified the Cybercrime Convention in their national jurisdiction [16].

The fact that a new kind of criminality occurred with the help of new technologies called for the Cybercrime Convention. The risk of a new kind of criminality was that the new technologies can support conventional crimes and make it easier, and even establish new crimes. Consequently, the necessity for such a treaty was given in order to combat efficiently computer criminality together. The good and quick

cooperation between the nations seemed to be essential in order to be effective. The nations agreed to protect the confidentiality, integrity and availability of IT systems.

The convention is structured in three sections. One section defines the offences which have to be declared as criminal in the national jurisdictions and the next one describes how the crimes should be pursued, so called the law of procedure. The last section is about international cooperation. [14]

The articles two to ten of the Cybercrime Convention describe the offences which have to be declared as illegal.

Art. 2 and Art. 3 Illegal access and interception

The second article mentions **unlawful access** to a computer system as an offence. The overcoming of a security precaution can be called as a prerequisite for the mentioned offence.

The **illegal interception** of data is declared as unlawful in Art. 3. The data has to be non open to the public and the interception also includes the electromagnetic emission.

Art. 4 and Art. 5 Data and system interference

In the fourth article **interference of data** is mentioned. Damage, deletion, alteration and suppression of data are classified as interference.

The next article (Art. 5) is about the declaration of the **obstruction of a system** as unlawful. The obstruction of a system caused by entering, transmitting, deleting, compromising, changing and suppressing of computer data is mentioned here.

Art. 6 Misuse of devices

The article about the **misuse of appliances** (Art. 6) refers to computer programs or similar appliances in order to commit the above mentioned crimes. It should be illegitimate to produce, sell, acquire, import and distribute such appliances, as well as to misuse access codes for unlawful access. This article only aims at the illegal use of such appliances and not at the legal one for IT security.

Art. 7 and Art. 8 Computer related forgery and fraud

Computer related forgery and fraud is covered by article seven and eight. These articles describe the usage of entering, alteration, deletion and suppression of computer data in order to obtain a pecuniary advantage or to claim that fake data is genuine.

After these articles, there are some articles about content related offences. Offences against copyright and children are declared as unlawful.

Art. 9 Offences related to child pornography

Additionally to the *Convention on the Rights of the Child* of the United Nations in Art. 9 of the Cybercrime Convention child pornography is also stated as a crime [73].

Art. 10 Offences related to infringements of copyright and related rights

The second content related offence is the one against copyright. Works of artists like paintings and installations, films as well as songs, fall under the copyright law for the protection of the works.

Art. 11 Attempt and aiding or abetting

In addition to the aforementioned crimes, Article 11 also states that **attempting and assisting or instigating** the crimes referred to is an offence. [14]

With these articles of the Convention of Cybercrime, the offences of **phishing**, **identity theft**, **software piracy**, **DDoS attacks** and **malware** are intended to be illegal additionally to the already specific mentioned ones.

Example

The case of the filesharing platform *The Pirate Bay* is an example for a European merged computer criminality case. The Swedish filesharing platform *The Pirate Bay* offered illegal streams of copyright protected works in the Internet. In the past already , the founders of *The Pirate Bay* were found guilty for abetment to copyright violations and the platform had difficulties with complaints for blocking their websites in different countries like Austria, Italy, Ireland and the Netherlands.
In 2017, *The Pirate Bay* even brought to trial before the Court of Justice of the European Union (Europäischer Gerichtshof, EuGH). The reason was a lawsuit of a Dutch foundation for copyright *Stichting Brein*. The judicial decision was that the filesharing platforms contravene against the copyright of protected works. The platforms support the violation of copyright of the users and therefore the platform is guilty of the violation of copyright. [26][1][48]
The administration of justice in this case on an international level was possible because of international treaties like the Cybercrime Convention. Otherwise every country would have had to decide the case on its own.

3.3.1 Supplementary Protocol

Additionally, to the Convention on Cybercrime, some nations signed a **supplementary protocol** which declares offences of **racist and xenophobic** nature as criminal. Germany signed the additional protocol in January 2003 and it entered into force in October 2011. In this supplementary protocol, propagation of material, threat, insult and offences against humanity with a racialist and xenophobic background is stated as criminal, as well as abetment and instigation of these crimes. [17][15]

3.4 General Data Protection Regulation (EU-DSGVO)

The investigation of a crime often intrudes into the sphere of privacy of the involved parties. In order to get information about a crime, the investigators have to examine the private life of suspects and analyse different IT systems or devices. These examinations violates the personal rights of the affected people. That is why data protection law has an outstanding position in an investigation. Despite the evaluation of private lives and digital devices the personal rights have to be sufficiently protected.

The European Union established the **General Data Protection Regulation (Europäische Datenschutzgrundverordnung, EU-DSGVO)** in 2016 and it entered into force in 2018.

The *General Data Protection Regulation* regulates the access to personally identifiable information in Europe. The access to personal data is determined in the fundamentals (Art. 5). The fundamentals state that the collection of personal data is liable to **earmarking and minimisation of data**.

That means for digital forensics that at an indemnity only the allowed data can be secured. The allowed data is determined by a search warrant and the secured data can only be used for the declared purpose. If a search warrant declares that the data of the cellphone should be collected, then only this data is enabled and not the data of an also seized computer, for example.

The fundamentals also state that the storage of the personal data has to provide a protection for **integrity and confidentiality** and the data is only allowed to be stored as long as necessary. The fundamentals regulate the **legality** of processing of personal data.

The legality means that if illegally secured and processed data is used in an analysis, the analysis cannot be used in the investigation.

The authorisation for the processing of personal data is constituted by Art. 6 of the EU-DSGVO for law enforcement and external service providers. [28][21]

Example

In Portugal the data protection authority *Comissão Nacional de Protecção de Dados* ascertained a violation of privacy in July 2018. The hospital *Barreiro Montijo* was sued for a violation of privacy. In this case, medical patient data was not only available to the medical staff but also to technicians of the IT system. Additionally, there were too many profiles of doctors in the system in comparison with the employed doctors. So, the hospital was found guilty and has to pay 400.000 euros. [45]

3.5 Strafgesetzbuch (StGB)

In the **German Criminal Code (Strafgesetzbuch, StGB)** [69] there are different paragraphs, which affect computer criminality and these paragraphs also implement the Convention of Cybercrime in the German jurisdiction. One of the most famous and controversial paragraphs is paragraph §202c StGB [64], also called the hacker paragraph.

Computer crime in the narrower sense is covered by various paragraphs of the German Criminal Code. Below we will look into the paragraphs which declare certain actions as illegal. The listed paragraphs are only a selection of the relevant laws for computer criminality. These paragraphs can be found in the sections *violation of the personal life and secret area*, *fraud and infidelity*, *forgery of documents*, and *damage to property* of the German Criminal Code. [28][69]

- **§202a Ausspähen von Daten** - This paragraph makes spying out of digital data a punishable offence. For the spying out, it is determined that the offender has to overcome security mechanisms in order to get the data. Paragraph §202a of the German Criminal Code is the equivalent to Art. 2 of the Cybercrime Convention. [62]

- **§202b Abfangen von Daten** - Paragraph §202b of the StGB covers the interception of data with technical tools. The interception of data is only referred to private data transmission and emission of a data processing system. So if the data is not private, this paragraph is not effective. [63]

- **§202c Vorbereiten des Ausspähens und Abfangens von Daten** - The preparations for the interception and spying out of data (§202a and §202b) is determined as illegal in paragraph §202c. These preparations contain the production, sale, procurement and propagation of access codes and computer programs in order to commit an offence. This paragraph is also called the *hacker paragraph* and there was furore about it among IT security experts. The *Federal Constitutional Court* rejected constitutional

complaints of IT security experts about the paragraph with the explanation that the intent for an offence is missing in their work [12]. Art. 6 of the Cybercrime Convention is its equivalent. [64]

- **§263a Computerbetrug** - Paragraph §263a is about computer fraud. Computer fraud is defined as the use of false and incomplete data or unauthorised usage or the change of data processing through an impact on the process or an inaccurate design of the programme. Even the preparation for such a crime is chargeable. This paragraph corresponds to Art. 8 of the Cybercrime Convention. [65]

- **§269 Fälschung beweiserheblicher Daten** - The paragraph is about the usage of an artificial or adulterated data or certificate. As well as the storage or the change of stored data in the way that it seems to be a certificate at perception. This adequate to forgery of documents (§267 Urkundenfälschung) in a digital way. [66]

- **§303a Datenveränderung** - The paragraph about the change of data means that the unlawful deletion, suppression, alteration of data and making data useless are chargeable. Even the trial and the preparation are indictable by §202c. [67]

- **§303b Computersabotage** - Computer sabotage is declared chargeable in paragraph §303b. Computer sabotage is defined as a disruption of a data processing. The disruption of data processing by means of crimes described by §303a and §202a in order to cause a drawback are mentioned. As well as the destruction, damage, disposal and alteration of data processing facilities or a data volume are chargeable. This paragraph corresponds to Art. 5 of the Convention of Cybercrime. [68]

These paragraphs of the German Criminal Code are a selection of laws regarding computer crime. More than these paragraphs are important in a trial about computer crime due to the complex construction of the law. But these paragraphs are often mentioned when talking about computer crime in the narrower sense. Some of these crimes are only pursued if a demand for prosecution is filed (§303c Strafantrag). [69]

When computer crime is allude to in the broader sense then, for example, paragraphs of the section *offences against sexual self-determination* in the German Criminal Code belong to computer criminality too. The paragraph **§184b Distribution, acquisition and possession of child pornographic writings** is such an example.

Paragraph **§184b** is not counted among cybercrime in the narrower sense but this paragraph is also an important one for the work of a forensic analyst. Child pornography cases are so common that the evaluation of the evidence is sometimes given to external digital forensics service providers and conventional computer scientists

who work as forensic analysts analyse the evidence [52][77]. For the investigation of evidence in a child pornography case, a forensic analyst needs further training in order to classify the material found. The further training involves the treatment of the Tanner stages. The Tanner stages enable the assignment of the children to different ages under 18. The forensic analyst has to classify the material by categories. [59][61]

Paragraph §184b declares the property, propagation or production of child pornographic works as unlawful. In the case of child pornography, there were legislation amendments and an analyst has to know these changes to mark out the works correctly in an expert assignment and to classify the pictures found in the correct way, for example. This paragraph of the German Criminal Code corresponds to Art. 9 of the Convention of Cybercrime. [61][53]

3.6 Urheberrechtsgesetz (UrhG)

The Cybercrime Convention declares in Art. 10 crimes against copyright as an offence. In the German jurisdiction, copyright and the offences against it are covered in the *Germany Copyright Act (Urheberrechtsgesetz)*. This law sets the work of artists under protection.

The unlawful use of a work is chargeable. Unlawful usage comprises the replication, propagation and publication of protected works without the approval of the creator as well as the editing and the reconfiguration of works for usage (§106 UrhG). [29]

With modern technology, the matter of copyright gets a new dimension. On the Internet the committing of an offence against copyright is simple. A digital copy of a work is easily made and anonymously distributed. So, to commit an offence against copyright is simple and many people are even often unaware of this indictable offence.

On the Internet, there are various film streaming platforms which are for free. These platforms show obviously illegally taped and copied films and series. Many adolescents and adults watch films on these platforms and are often not aware of the consequences. In some cases, the user is liable to prosecution for distributing protected works if the architecture of the streaming service is peer-to-peer.

3.7 Consequences for a Forensic Analyst

The knowledge of the legal situation of computer criminality is important for the work of a forensic analyst. A forensic analyst has to know the laws to observe them during the investigation and to designate the results of the expert assignment correctly.

In the demand for an expert assignment, the court requires the answer to an issue and the analyst has to understand the problem. Additionally, within the scope of an investigation, the laws have to be observed. A digital investigation operates with a big amount of high sensible data, because of this the data privacy has an exceptional

position in an investigation. Data protection has to be observed in the communication with the court and the storage of the data during and after the investigation. Analysts should keep up to date with legal changes and observe them in the investigation. The forensic analyst also has to comprehend a search warrant relating to the actions which are allowed by the search warrant. Because only if the work of the forensic analyst was legal, the evidence can be utilised in court.

The significance of the evidence can be weakened if an analyst disregards the laws during the examination of the evidence. A forensic analyst also could be guilty of the violation of privacy, if the analyst does not know the laws.

Thus, the forensic scientist must always be aware of the current laws in order to do the job well. A forensic analyst has to know the current legal situation but for an expert witness, even a better legal understanding is required. [28][14][2][69]

Negative Example

A corporate investigation in a matter of fraud is examined by an external service provider of digital forensics. The authority of the corporation gave the permission to the service provider to examine a specific folder in the post office box. The forensic analyst secures the complete post office box and analyses the secured emails.
In the report, the analyst demarcates suspicious emails and concludes the circumstances of the crime on the basis of all emails.
The customer of the expert assignment ascertains the violation of *General Data Protection Regulation* (EU-DSGVO) and proceeds against the digital forensics service provider. The forensic analyst is guilty of an offence against privacy during the work because the analyst did not consider the legal situation.

3.8 Further Reading

The exact wording of the legislative text can be found in the corresponding statutes like [69], [15] and [21], for example. A good advanced essay about the legal challenges with digital forensics can be found in the dissertation [34] and a report about the German situation of cybercrime can be found in the annual report “Bundeslagebild Cybercrime” [11] of the German Federal Criminal Police Office.

3.9 Summary

In this chapter, the relevant laws relating to computer criminality has been approached. On an international level, the *Convention of Cybercrime* of the Council of Europe regulates the international cooperation and unified legal situation to simplify the prosecution.

Additionally, the European Union established a common *General Data Protection Regulation* in 2018. The EU-DSGVO sets fundamentals for data processing.

The German realisation of the Convention on Cybercrime can be found in the *German Criminal Code* (StGB). In the German Criminal Code, there are some relevant paragraphs about the computer criminality. But only a few are mentioned in this chapter. The paragraphs are about computer sabotage, spying out and interception of data, computer fraud, alteration of data, and forgery of evidential data.

In addition to the paragraphs about computer criminality, paragraphs about offences against sexual self-determination are also covered in the German Criminal Code. The most important one for the work of a forensic analyst who works in law enforcement is paragraph *§184b* about child pornography because these cases are unfortunately frequent. For IT security experts in a corporation this paragraph a little less important than to forensic analysts who work for the law enforcement.

In the Cybercrime Convention and in the *German Copyright Act* (UrhG) offences against the copyright are covered. This statute book protects works of artists against the misuse of their works. These laws are important for a forensic analyst because these offences are so easily committed with the help of digital devices and these offences are so common.

The *consequences* of the laws for a forensic analyst are important. An examiner has to know the current legal situation in order to handle and evaluate the evidence in the right lawful way to preserve the significance of the evidence. In addition to that, the forensic analyst has to know the legal situation in order not to become an offender.

3.10 Review Questions

1. Which regulations are relevant to the legal situation of computer crime?
2. What is the challenge with digital evidence?
3. How does the presentation of digital evidence in court work?
4. What are the problems in the prosecution of computer crime?
5. What support the Cybercrime Convention for the subscribers and why was it needed?
6. What does a forensic analyst have to consider regarding the GDPR / DSGVO?
7. Which crimes from the StGB could be counted to computer crime?
8. Which consequences have a forensic analyst to consider in his work?

4 Computer Forensics

In this chapter, we will focus on the forensic examination of computer systems, i.e. laptops, desktops, and servers. During this chapter, a brief definition of computer forensics is given and a comparison to computer security is done.

Following, the process of a forensic examination of a computer is explained, focusing on the steps taken, e.g. identification, collection, examination and analysis, and documentation.

As with all the technical chapters in this lecture, also in this chapter a fictional forensic case will be introduced and taken as a guiding plan to explain the principles and techniques of computer forensics.

After the introduction of the case study, the steps of a forensic examination mentioned above are explained in detail, focusing on the forensic aspect but also recapping common knowledge in computer science, e.g. operating systems, disk structure, BIOS, and metadata.

At the end of this chapter, a quick summary of this chapter is provided as well as an entry point to the following chapter: Mobile Forensics.

4.1 Introduction

Computer forensics may be the most widely spread and applied branch of digital forensics. Most forensic cases tend to involve computers as main forensic evidence. This is no surprise due to the inseparable role computers play in our lives.

New technologies are developed, computers become faster and more powerful, giving attackers the opportunity to develop new methods for attacking and stealing information off computers.

Not only civil cases, like corporate espionage, are a great deal in forensics, but also criminal cases, for example, the possession and distribution of child pornography, are on the daily agenda of forensic examiners.

4.1.1 Definition

There are a lot of different definitions for **computer forensics**, some provided by official agencies like **CERT** (Computer Emergency Response Team) or ones provided within forensic books. We will take following definition for computer forensics.

Computer Forensics

The application of forensically proven investigation and analysis techniques, to collect, preserve and examine digital evidence from a computing device, in a way that is suitable for presentation in a court of law. The goal is to reconstruct forensic incidents while maintaining the integrity of all evidence and ultimately pin an incident to a perpetrator. [2]

A forensic examination does not always have to be a criminal one as mentioned above, but even in corporate forensic investigations, the examiners follow strict procedures, i.e. chain of custody, evidence preservation, and documentation, so as if it would be presented in a court of law.

Following, a comparison between computer forensics and computer security is given, due to the often miss use of both terms.

4.1.2 Computer Forensics vs. Computer Security

Although, computer forensics is often associated with computer security, they are still different branches of computer science. Following, a brief comparison of computer forensics and computer:

- **Computer Forensics** - As the definition of computer forensics mentioned above states, computer forensics is primarily concerned with a proper collection, preservation, and examination of digital evidence from computers, usually after the occurrence of an incident that implies unauthorised access.
- **Computer Security** - In the case of computer security, the prevention of unauthorised access, i.e. the maintenance of confidentiality, integrity, and availability of computers lays in the main focus.

Nevertheless, computer forensics and computer security play hand in hand and present the different sides of the same coin. After an incident that involved unauthorised access, the forensic examination is of great importance for learning lessons about improving computer security against future events.

Following, the steps of a forensic examination in case of a computer system are explained.

4.2 Forensic Examination of a Computer

Digital forensics is a fairly new discipline in computer science, still, specific procedures, principles, and techniques have been elaborated by civil and government forensic examiners, which are mostly followed to guarantee results accepted by a court of law.

The four phases (identification, collection, examination and analysis, documentation), differ from source to source, mostly different names are used for the same process, but altogether the principle of a forensic examination stays the same. For this lecture, we dug up a lot of different sources and constructed a well suited summary.

Following, the four steps of a forensic examination of a computing device are introduced.

4.2.1 Identification

The identification phase is always the first step of a forensic examination no matter what kind of investigation it is, corporate or criminal. This phase is normally carried out, in case of a criminal investigation by the police, by the first responders of the crime scene unit. In case of a corporate investigation, a specialised group mostly called **Incident Response Team** carry out the identification phase.

The identification phase does not necessarily require fully trained forensic examiners, and can also be carried out by normal first responders or employees with basic understanding of digital evidence.

This step involves the seizure and the marking of all elements that are going to be forensically examined later on, photographs of the incident scene and notes are taken as well.

An important decision to make during this phase is whether to pull the plug on the computer or leave it on. In digital forensic jargon this is called **Live Forensics vs. Post-Mortem Forensics**. This is why it is recommended that a forensically trained team should handle cases like this.

A forensic examiner should know that, on one hand, leaving the system on for a live forensic examination may alter data and wipe potential evidence, or even alert the intruder of such an investigation, but also enables the seizure of volatile data like RAM and running processes. On the other hand, pulling the plug may destroy volatile data, but will preserve the state of the machine as it was after the incident and will ensure no further alteration. [22]

After making that decision, a forensic examination is then proceeded with the collection phase.

4.2.2 Collection

After the identification phase comes the collection phase. For later examination, all identified evidence, i.e. computer, must be seized without damaging or altering the original source and state.

Most results of forensic examinations are presented in a court of law, that is why any illegal seizure or improper methodology used could affect the admissibility of the evidence and render it useless in a court of law.

All methods used to seize and collect digital evidence, must be forensically sound and verifiable by third party examiners.

Two arts of of data collection exists, **logical and physical**. In case of a physical acquisition, a *bit-by-bit* copy of the seized storage media is made. In case of a logical acquisition, a *logical image* of the storage media is captured. Both methods require *Write-Blockers* to prevent the source from being modified. [22]

Hash values of original and duplicated data are made to be compared, which verifies the duplication process.

While collecting evidence, an examiner must be aware of the *order of volatility* which was introduced in a previous chapter, and should always start collecting the most volatile data first. The order of volatility of data on a computer goes as following:

- Registers and Cache
- Network State
- Running Processes
- Kernel Modules and Statistics
- Main Memory
- Temporary files on disk

Most tools for forensic evidence collection are software based and need training for correct usage. [22]

The next phase is the examination and analysis phase, which is thoroughly explained below.

4.2.3 Examination and Analysis

In the collection phase, the evidence seized is only random data, and no context exists, yet. The examination and analysis phase is the phase, where evidence collected before is interpreted and information are extracted. Specific forensic methodologies exist for this phase, and require a fully trained examiner. An examiner will use the copies of the original evidence made before for this phase, and under no circumstance the original data.

Again, software tools, i.e. for restoring deleted data, to aid examiners in this process are available, all must be forensically reliable and their correctness must be ensured.

Typically, a forensic examination contains two approaches: looking for **something unknown in something known**, and looking for **something known in something unknown**. The before mentioned approaches, are explained below:

- **Unknown in Known** - In this approach, an examiner would look for infected programs, erased documents, browser history, or chat/calls history.
- **Known in Unknown** - During this approach, an examiner would look for meaningful information in unstructured data like: URLs, emails addresses or cryptographic keys through the use of carving techniques. This seemingly random data is assembled and used to reconstruct events.

Both approaches and their results are aggregated and contribute to finding facts about the incidence scenario, attackers, locations or other related facts.

This phase, in contrast with the collection phase, can not be conducted by non-experts. Examiners must have deep knowledge in the branch of digital forensics and be specialised in computer forensics. [22]

Last but not least, the documentation phase, which is one of the most important phases, is explained next.

4.2.4 Documentation

To withstand a formal investigation by third parties and be accepted in a court of law, each forensic examination has to be thoroughly documented and reported. This phase is crucial and is conducted by the examiner to ensure a detailed description of all results and steps conducted during the examination.

A forensic examination report contains following information:

- **Identification Phase** - Descriptive information about where evidence was found, or who it was received from, to uniquely identify all seized data.
- **Collection Phase** - Information about the collection phase, i.e. who did the examination, when was the examination conducted, which tools were used, original data hash, etc.
- **Examination and Analysis Phase** - Detailed information about the examination phase, e.g. description of examined media, which tools were used.

With a forensic report, a third party examiner can reconstruct and understand all steps taken by an examiner and independently verify the correctness of the investigation if needed. [22]

4.3 Case Study

For each technical chapter in our lecture, a case study, e.g. a fictional forensic incident, has been constructed. This forensic incident will help with the explanation of the

forensic methodologies and aid the student in understanding the principles of digital forensics both theoretically and practically.

For this chapter, a forensic incident involving a company hired by the government is introduced. A detailed look at the case study, e.g. the scenario, involved individuals, entities relevant for the forensic investigation, and the problems that the investigators are confronted with, is given below.

4.3.1 Scenario

Alice's company is specialised in disposing of hardware used by the government. The process of disposing the hardware correctly, e.g. without leaving traces of data on the hardware, is complicated and strictly followed by the company. Bob is responsible for shredding the data on mass storage devices. In his laboratory, hundreds of hard drives and USB sticks are daily shredded and disposed of. After the shredding of data on the mass storage devices, the hardware is destroyed using electromagnetic waves, which renders them useless.

Bob is not happy about his salary and after a discussion with Alice, it was clear that no raise in salary is possible. Bob had a brilliant idea, on how to get a little extra money on the side. Bob decided to sell the hardware to a third party, Dave.

Dave and Bob came to an agreement, and Bob started keeping 10% of the hardware each day and would then deliver them to Dave. Charlie, the person in charge of disposing the hardware, had noticed a significant decrease in the amount of hardware disposed of, while the inventory stayed the same. Charlie confronted Alice and told her about the inconsistencies he found.

Meanwhile, Dave had already sold a few hard drives to a shady black market hacker, Eve. Eve has successfully reconstructed some shredded data off the hard drives she bought, which contained top secret government documents.

Alice and Charlie confronted Bob about the missing hardware. He denied any involvement in the missing hardware. In the meantime, the documents have been published by Eve and aroused the attention of government agent Grace.

Grace is a government agent specialised in digital forensics and has been given the task to uncover the fiasco. Alice's company is now under a criminal investigation by the government, but Alice wanted to make sure everything is done fairly and hired a private forensic investigator as well, Frank.

Grace and Frank work hand in hand to uncover the mystery and to find the person responsible for the illegal selling of hardware.

This case has both criminal and corporate aspects, i.e. criminal because the company is hired by the government and corporate because this incident impairs the reputation of Alice's company.

Bob realised that he is the primary suspect, but luckily for him, he had concealed all his steps while communicating with Dave, or so he thinks. Bob used steganography to hide text files inside of pictures, which he then sent to Dave via email. Along with that,

he deleted the pictures from his machine by using the Windows shortcut "Shift+Del". Since the first communication with Dave, Bob has visited multiple websites to find out how much used hard drives are worth, then he emptied the browsing history through the browser. Bob kept a protocol of all sold hardware, including hardware ID's, price sold for, time and date. This protocol is a Word document which he copied to an external USB drive after he was confronted by Alice and Charlie.

Bob's laptop has been confiscated by the forensic examiners and is in a turned on state.

Following, all individuals involved in the scenario and their description is provided.

4.3.2 Individuals

Individuals involved in the forensic case and their roles, are listed below:

- **Alice** - CEO of the company.
- **Bob** - Shredding Officer, primary suspect.
- **Charlie** - Disposal Officer.
- **Dave** - Hardware merchant.
- **Eve** - Black market hacker.
- **Grace** - Government agent (forensic investigator)
- **Frank** - Civil forensic investigator (third-party hired by Alice).

All mentioned individuals play an important role in this forensic examination. Following, all entities, i.e. digital evidence of interest, are listed below.

4.3.3 Entities

Bob's computer is the primary piece of digital evidence available in this case. The computer had been seized and is in a turned on state. The computer has the following technical specifications:

- **State** - Powered on.
- **Operating System** - Windows 10.
- **Storage** - 500GB HDD and 256GB SSD.
- **Memory** - 8GB of RAM.
- **Connectivity** - Internet connection through WLAN.

During an interrogation, the password for Bob's PC has been seized, so full access to the computer is privileged. Next, the problems arising and facing the forensic investigators are listed.

4.3.4 Problems and Goals

Frank and Grace have a few decisions to make, which are substantial for the forensic investigation. The first decision is whether to use *live forensics* or *post-mortem forensics*. The pros and contras of both approaches have been explained previously.

A notable problem is the missing USB stick, that Bob copied his protocol on. This USB was not confiscated and can therefore not be accessed. Traces of attached hardware can still be found on the host system, which might help the forensic examiners.

Finally, the main goal of the investigation is to find indisputable evidence which proves that Bob was in contact with Dave.

After the explanation of the case study and all relevant information, it is time to start the forensic examination. In the coming chapters, the student is accompanied by the two forensic investigators Frank and Grace in this forensic examination. Important forensic principles are explained, tools and methods are listed, and a recap of common knowledge in computer science is briefly summarised when needed.

4.4 Phase 1: Identification

After the explanation of the basic principles of a forensic investigation, let us start the investigation of the above mentioned case study.

Grace and Frank will lead the way and start with the identification phase. During this phase, an important decision is made, e.g. live or post-mortem forensics. The decision will lead us to the explanation of two important computer components, i.e. **CMOS** and **BIOS**.

As soon as Grace and Frank are done identifying all relevant digital evidence, e.g. Bob's computer, taking pictures of the computer and the environment it was confiscated at, they can continue with other important steps.

Moreover, a *chain of custody* is built to make sure, that all items relevant to the investigation are always available. The digital evidence identified as relevant is then collected and secured, during this, the *dual control principle* is always followed to make sure that all actions taken can be verified by two investigators. [22] [2]

4.4.1 Live Forensics vs. Post-Mortem Forensics

As explained before, both approaches of forensic investigation, e.g. live and post-mortem, have their pros and contras. In our case, communication protocols, e.g.

network state, is of great importance, because the investigators are trying to find evidence that Bob was in contact with Dave.

As we know, the network state of a computer, is one of the most volatile data. To make sure this volatile data is not lost, Grace and Frank decided to use the live forensics approach, i.e. keep Bob's PC turned on, and start an investigation on the system directly.

There are a lot of tools available for live forensics, most of them are images which need to be booted from, to get access to the tools and to the operating system. The process of booting a live image prerequisites access to the BIOS of a computer.

In the exercise, we will introduce a forensic tool used for live forensics and explain practically how to use it. For now, it is important that everyone understands what a *CMOS* and a *BIOS* is. So, following an explanation of these components is given.

CMOS and BIOS

CMOS, which stands short for Complementary Metal Oxide Semiconductor, is a hardware chip which every computer has.

Complementary Metal Oxide Semiconductor

The CMOS, sometimes referred to as Real Time Clock (RTC) or Non-Volatile Random Access Memory (NVRAM), is a hardware chip including firmware which saves important configurations for a computer.

Information stored by the CMOS is **non-volatile**, e.g. kept even after shutdown. These vital information are usually the boot order of a computer, date and time, amount of installed memory and other settings. The CMOS is the first responder when a computer is turned on, and without the information stored, or with miss configured CMOS settings, a computer would not be able to boot properly and would not know how to communicate with basic hardware components like input/output devices or RAM.

For a forensic examiner, the information stored in the CMOS is often the first bit of information an examiner can collect. For a forensic examination, the date and time of the examined system, as well as the connected hard drives, are examples of important forensic evidence.

BIOS, short for Basic Input/Output System, is the lowest level of software, is motherboard specific, and typically relays within a read/write flash memory.

Basic Input/Output System

The BIOS is the lowest level of software, also called firmware, that enables an interaction to the hardware components of a computer. [27]

Critical information like boot order, password protection and other are accessed through the BIOS. Accessing the BIOS is one of the first steps, a forensic examiner would initiate. Once the BIOS is accessed, settings like the boot order or security modules can be altered. An examiner can then check whether hardware components like Wireless Modems, Bluetooth Chips or TPMs, short for Trusted Platform Modules, are available. Sometimes, if a live forensic analysis is needed, it is necessary to boot up the system from a different source, like a live USB with pre-installed forensic tools, which is done through the BIOS.

Much like the CMOS, the BIOS is accessed by pressing a designated key during boot, this key is vendor specific. Expert computer users use passwords to protect their BIOS, many vendors ship their BIOS chips already protected by a password. An important first step for a forensic examiner is to prepare a list of vendor BIOS passwords; typically, a Google search for the BIOS vendor is enough, and then using these found passwords to access the BIOS. [27]

Forensic Examination of a BIOS Chip

During forensic examinations, BIOS chips are largely ignored, even though they are the perfect place for hiding data. No established forensic procedures or tools exist, that aid an examiner during the examination of a BIOS chip.

In this section, we will describe how to use common forensic tools to manually inspect a BIOS, particularly finding hidden data using file carving and searches based on regular expressions.

To start analysing a BIOS chip, we need an approved BIOS flashing tool. A MS-DOS compatible flashing tool is the *Caldera Dr-DOS*. Proceed to create such a compatible boot disk.

For later use, we want to copy the *Uniflash* program (UNIFLASH.EXE) and all its components to our boot disk. One can now boot the machine from the created boot disk. Execute *UNIFLASH.EXE* and create a backup of the seized BIOS and save it as *BIOSevidence.bin*, which will create a forensic image of the BIOS. Copy the created image to your workstation.

On your workstation and for **Award BIOS** chips only, use *AwardMod* to extract all modules within the image created before. Store them in a directory called *BIOSevidence*.

Within your workstation, use forensic tools like *Foremost*, *EnCase*, and *ILook* to examine the created BIOS image and the extracted modules. The file *D3VA1323.BIN*

should be of special interest to you. The forensic examiner should be looking for text, file headers, and regular expressions.

D3VA1323.BIN is 128K in size, and can be therefore also examined manually using your favourite hex editor.

If the person hiding data on the BIOS chip is really sharp and skilled, it will be hard finding any hidden text, and if found, it would be hard classifying it as important.

To avoid wasting unnecessary time looking for something that might not be there, get your hands on a clean copy of the BIOS chip, e.g. obtained from the manufacturer, and use a hex editor to compare the seized copy with the clean copy. This will aid the examiner in finding discrepancies.

Following this procedure, the forensic examination of a BIOS chip is done, and possible evidence is seized. In the Chapter *Anti-Forensic*, the other side will be explained, i.e. the process of hiding data within the BIOS chip. [27]

Grace and Frank have now access to the BIOS, and are able to boot their live forensic image. The computer is then booted from this image, providing an operating system including all forensic tools they need as well as read-only access to the computers storage.

4.4.2 Securing Digital Evidence

After the identification of all important digital evidence, it is important to collect these evidence and secure them so they are protected from third party tampering. For that, Grace and Frank have access to a forensic laboratory, and the access to this laboratory is limited to Grace and Frank.

At all time, Grace and Frank both have to be in this laboratory, and at no time should only one investigator have access to the evidence. In digital forensics, this is often refereed to as the *double verification principle*.

Grace and Frank have finished the first phase, i.e. the identification phase. They have successfully identified all relevant evidence, they documented the confiscation process, a decision on which forensic approach to use was made, and the evidence was securely collected and stored in a laboratory which only both of them have access to.

Now that the identification phase is over, the collection phase can begin. Following, the collection phase of our forensic investigation is explained.

4.5 Phase 2: Collection

Grace and Frank have access to the data stored on Bob's computer thanks to the live forensic image they booted the computer from. The collection phase, as explained

before, involves the acquiring of data present on the storage of the computer without tampering or altering it if possible, to analyse later in the examination phase.

4.5.1 Operating System Determination

One of the first steps in the collection phase is to determine what operating system is present on the confiscated computer. This varies from operating system to operating system, but with the live forensic image that Grace and Frank are using, a few steps can be taken to determine OS version and patch level.

In Windows, there is usually a file called *MSDOS.SYS* which indicates the operating system version, under Linux it is possible to determine the kernel version using the command *uname -a*.

4.5.2 Order of Volatility

After the determination of the operating system used by Bob's computer, e.g. Windows, Grace and Frank have to pay attention to the order of volatility explained before. The network state of Bob's computer is important for our investigation, because the investigators are trying to find evidence of a communication between Bob and Dave. Information about attached hardware is not volatile, and is usually kept even after shutdown. In case of a Windows computer, the information about attached hardware is kept within the **Registry**. [2]

Windows Registry

If normal or expert computer user, hacker or forensic examiner, you have probably heard of the Windows registry. The Windows registry is basically a big database, storing all kinds of important information for a Windows operating system like installed programs, security profiles, hardware drivers and much more.

For example, whenever a new program is installed, a new entry in the Windows registry is made, stating important information about this installed program, where to find its data, what access rights it has and so on.

For a forensic examiner, one of the first steps is to analyse the Windows registry and specifically look for the following entries: security, software, system and SAM. [47]

Forensic Examination of Windows Registry

The Windows Registry is basically a big pile of evidence, just waiting to get collected by a forensic examiner. The Windows Registry can be viewed as a database storing configuration information about everything, e.g. users, hardware, and software.

Information stored within the Registry can be crucial for answering forensic examination questions like who,what where, and when.

Firstly, let us take a look at how the Registry is built. In all Windows versions, the Registry is divided into *Hives*. There are five *Registry Hives*:

- **HKEY_USERS** - Contains all the loaded user profiles.
- **HKEYCURRENT_USER** - Profile of the currently logged-on user.
- **HKEYCLASSES_ROOT** - Configuration information on the application used to open files.
- **HKEYCURRENT_CONFIG** - Hardware profile of the system at startup.
- **HKEYLOCAL_MACHINE** - Configuration information including hardware and software settings.

Basically, the structure of the Registry is similar to the Windows directory/subdirectory structure. So, navigating through the Registry is as easy as navigating through the file system, as long as one knows where to look for what.

Each *Hive*, also referred to as *Key*, has *Subkeys*, which can contain *Sub-Subkeys* or actual *Values*. Values are mostly 0 or 1, for off and on respectively, or more complex like hexadecimal values.

To access the Registry of ones own PC, no forensic tools are needed, simply press *Super+R* and type *regedit*.

For a forensic examination, the following information can be found within the Registry:

- Users and the time they last used the system.
- Most recently used software.
- Any devices mounted to the system including unique identifiers of flash drives, hard drives, phones, tablets, etc.
- When the system connected to a specific wireless access point.
- What and when files were accessed.
- A list of any searches done on the system.

Let us get technical, and look at some of the most important *Hives* and *Values*. Evidence of wireless access point connection can be found under: *HKEY_LOCAL_ MACHINE/SOFTWARE/Microsoft/Windows NT/CurrentVersion/NetworkList/Profiles*. There, a list of GUID's of wireless access points the machine has been connected to can be found.

Recent documents that were recently opened, are sorted by the extension and can be found under: *HKEY_CURRENT_USER/Software/Microsoft/Windows/Current Version/Explorer/RecentDocs*. Traces of files with the extension *.tar* can be an indicator for malicious activity, because the Windows OS does not usually support *.tar* files.

Another interesting address in the Windows Registry is the TypedURLs key, which can be found under: *HKEY_CURRENT_USER/Software/Microsoft/Internet Explorer/TypedURLs*. Normally, users should not be using Internet Explorer, we all know why. But when Internet Explorer is used, all URLs typed by the user are saved in the above mentioned key.

For network forensics, the IP addresses a computer has interfaced with, are of interest. The last 25 IP addresses of a Windows PC can be found under: *HKEY_LOCAL_MACHINE/System/Services/CurrentControlSet/services/Tcpip/Parameters/Interfaces*. For intrusion detection purposes, this *Hive* is a gold mine. IP addresses, subnet mask, DHCP settings and many other information can be found here.

Other important information like mounted devices and startup applications can be found in the Windows Registry. [47]

What each of the entries contain and why they are important for a forensic examiner will be shown in a practical exercise.

Software based tools are available to acquire and analyse network data of computers, or to analyse the *Registry*. Practical use of these tools will be conducted during the exercise.

Due to the live forensics approach, the investigators need to forensically image the collected evidence, e.g. the RAM of the computer, and the storage devices attached to it.

The process of correct forensic imaging and the different types are explained below.

4.5.3 Forensic Imaging

During the collection phase, no matter if live or post-mortem forensics is used, a forensic imaging of all evidence storing data is done. This process must be forensically sound and proven and assure no alteration of data during the process.

The investigators have full access to the computer and must now decide whether to create logical or physical images of the evidence. Generally speaking, whenever the option to use physical imaging is available, it is suggested to use it. Physical imaging, as explained before, ensures access to hidden and deleted data that lays within the **unallocated space**.

Grace and Frank will now use their live forensic tools to create a physical duplication of both storage devices, e.g. HDD and SSD, as well as from the RAM.

Disk Structure

To better understand the process of forensic imaging, e.g. cloning, and how to handle the different components of a mass storage device, a quick recap of **disk structures** is given.

The word disk is used to refer to a physical storage device. Such a storage device can contain **volumes** and/or **partitions**. From the forensic aspect, it is important to understand the difference between volumes and partitions.

The term partition, although often interchangeably used with volume, is used to refer to a section of a disk with a specific size that is set at creation time.

Partition

A partition is a sectored, unformatted, fixed size space in a disk.

A partition is not necessarily formatted, and does not contain a **file system**. For a forensic examiner, the examination of all partitions is necessary. Some partitions might be **hidden**, others might be **bootable**, thus containing important information for a forensic analysis.

A hidden partition might contain data, that a perpetrator is trying to hide, which can be easily done using *anti-forensic* tools. A bootable partition, is a partition that a computer is able to boot, e.g. start an operating system from. From such a partition, a lot of information about the operating system can be concluded, i.e. version.

Another important forensic aspect is the **partition gap**. The partition gap is the space of a partition that is reserved for an operating system or for use if a partition is running out of space. More to what exactly the operating system reserves it for in a bit.

Mostly, when dividing a disk into partitions, some space between the sectors is left unused, which results in *unallocated space*. Unallocated space is usually hidden from the user by the operating system and is therefore a great place for hiding data.

All disk analysis tools provide forensic examiners easy access to all partitions including partition gaps, thus making it fairly simple to examine the unallocated space and to carve out files that are hidden there. [2]

In relation to partitions, two important terms often occur, e.g. **MBR**, short for Master Boot Record, and **GPT**, short for GUID Partition Table.

- **Master Boot Record (MBR)** - The MBR is the first 512 byte sector of a partitioned disk, which holds information necessary to boot a computer, like the number of partitions on that disk. For obvious reasons, a forensic examiner must know how to inspect the MBR and how to find out if it was manipulated. An attacker might change the MBR in a way, that it leaves out a partition, which results in a hidden partition. If a forensic examiner is not familiar with

the MBR, the forensic analysis might be incomplete. MBR is very limited in its structure, for example, MBR disks can only hold four partition, and has limits in how large the disk may be, e.g. 2 TB. [2]

- **GUID Partition Table (GPT)** - Due to the limitations of MBR, GPT was introduced. GPT, like MBR, stores information about the partitions existing on the disk. A GPT formatted disk is much more complex than its legacy predecessor and is therefore harder to understand. GPT can hold unlimited partition, in a Windows operating system it is limited to 128 partitions, and supports much larger disks, e.g. 18 Exabytes. A forensic examiner must be able to forensically examine a GPT formatted disk, because most modern day computers tend to use it instead of MBR. There are tools which aid forensic examiners in analysing GPT disks, like the Sleuthkit. [2]

As mentioned above, the terms volume and partition are often mixed and used to describe the same thing. But here, we want to clearly separate both terms.

Volume

A volume is the part of a partition containing a specific file system with a fixed size.

A volume, in contrast to a partition, is the part of a disk that is formatted and contains a file system as well as a size. This part of the disk, is the part that the user interacts with, and is typically, at least in the Windows operating system, denoted with a single letter, for example ”C”.

Multiple volumes can be stored on a single disk, and the operating system keeps track of where volumes are stored. When focusing on Windows operating systems, volumes are of great importance for a forensic examination. Since Windows XP, the operating system creates periodic backups of the volumes, so called **Volume Shadow Copies**, which function as restore points for the user.

For a forensic examiner, these shadow copies are often a good source of information. By restoring the operating system to a previous point, a skilled examiner can find the differences between the current and the previous state of the computer. With these information, the examiner is then able to recreate and understand the forensic incident. [2]

Following, a quick recap of file systems is given.

File System

As mentioned above, a volume is a part of a disk that contains a file system.

File System

A file system is a structured volume and defines how data is stored.

We will take a closer look at **FAT**, short for File Allocation Table, which is one of the oldest file systems and the most commonly used across different operating systems.

There are lots of file systems, some of them are operating system specific, while others tend to be used for external hard disks instead of internal ones. In this section, we will introduce four file systems, FAT, NTFS, EXT and HFS. The first two are meant for Windows operating systems, and we will explain those in detail.

- **File Allocation Table (FAT)** - FAT which was developed by Microsoft in 1967, is a file system that keeps track of the allocation status of clusters on a hard drive. This file system performs faster than its alternatives when it comes to smaller drives, e.g. less than 10 GB, and there are four possible FAT entries: allocated, unallocated, end-of-file and bad sector. For a forensic examiner, it is important to understand that files could be hidden in the unallocated space sector. Unallocated space can be used to hide bits and pieces of data, but most modern forensic tools are able to automatically carve out files that are hidden in the unallocated space. [2]

- **New Technology File System (NTFS)** - NTFS is a file system developed by Microsoft and introduced with Windows NT. NTFS quickly became the standard for the following Windows versions and had features which made it better than FAT, for example journalling, security access control lists and better performance. In NTFS, each file has three timestamps, one for each of the following: created, modified and accessed. [2]

  For a forensic examiner not only the timestamps are of value, but also the fact that ADS, short for Alternate Data Streams, exist. More to ADS, what they are and do will be explained in a later section.

  In a NTFS file system, there is a database that holds information about all directories and files, this database is called MFT, short for Master File Table. For the file system, the information contained in an MFT entry are important. Information like timestamps, size and access control are specifically interesting for a forensic examiner.

- **Hierarchical File System (HFS)** - HFS and its successor HFS+, are file systems designed for Apple's Mac OS. For a forensic examiner, it is important to know that there are five special files in this file system, for example the startup file, which is like the boot sector in FAT, where important information for an

examination may reside. Important to mention is also that HFS implements journalling, which is a way of recovering files after a crash. [2]

- **Extend File System (EXT)** - EXT is a file system used by most Linux operating systems. It consists of four different types: ext, ext2, ext3 and ext4. The file system is inspired by the metadata structure used by UFS, short for Unix File System. [2]

After the quick recap of volumes, partitions, and file systems, another important step during the collection phase needs to be explained, i.e. file hashing.

File Hashing

During the collection phase it is necessary to create hash values for all files of the examined computer, that means of all files, documents, images and others.

File Hashing

Hashing is the application of mathematical functions on large input data to reduce it to a fixed size output. [22]

This is not only important to cross reference it with the original data to verify its integrity, but also to cross reference it with databases and look for hits, e.g. finding the same hash already stored in the database. There are special databases that for example save the hash values of default Windows files.

A forensic examiner can cross reference the ones available with the default ones to quickly identify a corrupt or altered file. Another use is when it comes to images or videos of disturbing nature. A forensic examiner can cross reference the hash values with a database that collects those kinds of videos and images, and with this, being able to find a file that is already known. This spares a lot of time and is enormously quicker then manual comparison of media.

Our forensic investigators have made forensic copies of the evidence provided, they understood the difference between volumes and partitions. Also, they got a little insight into file systems and determines the operating system of Bob's computer. Considering the order of volatility, they have created hashes of the original data to use it as a later verification.

Now, Grace and Frank have seized and collected all relevant evidence and are ready to analyse and examine them. The next phase will be the examination and analysis phase.

4.6 Phase 3: Examination and Analysis

During the examination phase, Grace and Frank will try and analyse the collected evidence and look for two types of evidence:

- **Exculpatory Evidence** - Evidence which might exonerate a suspect.
- **Inculpatory Evidence** - Evidence that incriminates a suspect.

To ensure a structured analysis and examination phase, let us take a look at the different types of data that Grace and Frank might encounter, e.g. active, archival, and latent data.

4.6.1 Active Data

Active data is data that can be seen and accessed without the use of any special tools. This includes user files, operating system files, and program files.

Active data is the easiest to examine and usually is the first place an investigator would look for evidence.

For our investigation, browser history files are of great importance, as well as information about attached hardware. After a quick analysis, Grace and Frank find cached websites, and traces that indicate an attached USB thumb drive within the Registry. These cached files indicate that Bob was browsing for keywords that incriminate him, i.e. used hardware prices. The Registry entries suggest that a thumb drive was attached to the computer, which prove that Bob's statement, stating that there was no USB drive, is false.

For every forensic examination, **log files** are of great importance. Log files are active data that stores user activity. Below, a quick explanation of log files within a Windows computer, is given. [22]

Log Files

In a Windows computer, there are three main types of log files: System, security and application. These log files are event based, e.g. whenever an event occurs, an entry is made in the corresponding log file. A Windows server contains additional log files based on its functionality.

A forensic examiner must know where to find those log files and ideally how to read and extract information from them. Each log file is made of a header and a body, whereas the body being the main source of information for a forensic examination.

In other operating systems, i.e. Linux or Mac, there are also log files of interest for a forensic examiner. More to log files in different operating system is provided in the exercise. [22]

4.6.2 Archival Data

Archival data is, as the name suggests, data that has been archived, e.g. backed up and stored. Most archival data is not present on the current computer, but rather on backup tapes, CDs, floppies or external hard drives.

Finding traces of archival data is hard, but finding an indicator that files have been copied to an external device are easy, e.g. using the Windows Registry.

Using forensic tools, Grace and Frank find indications of an external USB thumb drive that was connected to Bob's computer. The fact that a USB device was connected to, and that files were copied to it, indirectly incriminates Bob due to the fact that he is denying the presence of such a device. [22]

4.6.3 Latent Data

Latent data is data that typically is not fully available, e.g. which needs reconstruction using specialised tools. This includes data that has been deleted or overwritten.

Data that has been deleted is typically not really deleted, but rather the operating system marks the space as available, e.g. overwrite able.

Another type of inaccessible data in a Windows computer are **ADS** (Alternative Data Streams). Next, a little explanation of ADS is given. [22]

Alternative Data Streams

ADS was introduced in Windows operating systems to comply to resource forks used by HFS. Basically, ADS store information about a given file, for example author or title, but not in the main data stream, rather in an alternative stream.

Since Windows XP SP2, ADS where used to assign each file a Zone Identifier. The zone identifier is a number, that indicates where a file came from, for example from the internet, from an external hard drive or others. Based on the zone identifier, the operating system would warn the user if they tried to execute these kind of files.

A forensic examiner can look for hidden data in ADS and classify those by source, which is often important for understanding the forensic incident.

Grace and Frank can use their forensic tools to reconstruct deleted files, which include emails that Bob has sent to Dave.

The process of reconstructing deleted files is a complicated process, which is important for every forensic investigation and is therefor explained thoroughly below. [2]

Example: The Craigslist Killer

Philipp Haynes Markoff, born on February 12 of 1986, was a successful medical student at the Boston university, charged with armed robbery and the murder of one Julissa Brisman.
He used a platform called *Craigslist* to offer his services, luring in unaware girl to abandoned locations, to then rob and possibly kill them.
All in all, the police suspected him in three cases of armed robbery, one of them ending deadly. The first one occurred on the 10th of April near a Hotel in Boston, where Trisha Leffler, an escort, was found bound, gagged, and robbed at gunpoint.
The second one was Julissa Brisman, who thought that Markoff offers a massaging service. She was found dead on April 14th.
Corinne Stout, an exotic dancer, was the last victim which he attempted to rob on the 16th of April.
The police suspected the same person, because of the similar traits of the crimes. Computer Forensics was used, including the analysis of CCTV footage, cell phone activity and email evidence, which ultimately incriminated Markoff leading to his arrest.
After his arrest, a semi-automatic gun was found in his apartment, as well as duct-tape and restraints, which made him look even more guilty.
Even though pleading innocence, waiting on his trial, and the fact that his fiancee has called of the wedding, Markoff has attempted suicide a grand total of four times, the last one being successful.
Markoff was then found dead on August 15th of 2010, on day after his wedding was supposed to take place. [9]

File Carving

For a forensic examination, file carving is an important step and is always initiated.

File Carving

File carving in digital forensics is a technique to restore deleted or fragmented files based on their headers. [76]

Tools like Foremost reconstruct these fragmented or deleted files based on their headers and footers. Once a header is found, the tool will look for an indication of the size of that file, then it will ”carve out” until the size is fulfilled and then look for an appropriate footer at the end, if one is found the file is reconstructed, otherwise it is dropped.

File carving can be applied on unallocated space as well as on file slack. Following, a little introduction to unallocated space and file slack. [76]

- **Unallocated Space** - For an operating system, the space on a disk is either allocated or unallocated.

  On one hand, allocated space is the space on a disk that is used by the operating system. Unallocated space on the other hand, is the space on a disk that is not used by the operating system, but that does not imply that it is empty, it has only been marked as empty.

  When imaging a disk, a forensic examiner has to choose between physical or logical imaging. The advantage of physical imaging is that the unallocated space of a disk is duplicated as well, which gives the forensic examiner the opportunity to inspect it. Unallocated space usually contains data that the user has deleted, but was not yet overwritten by new data.

  Data stored in unallocated space is not always in tact, and techniques to reconstruct them are needed, e.g. file carving. [2]

- **File Slack** - File slack as mentioned above happens due to how operating systems section the attached storage devices.

  A disk is sectioned into clusters, typically in 4096 byte clusters. Each cluster is then divided into sectors, usually 512 byte sectors. So when a file with only 12 bytes is stored in a sector, 500 bytes are left free. The operating system would not save another file in these free 500 bytes, but rather use a new sector.

  Therefore, empty space is left at the end of the file resulting in slack. For a forensic examiner, file slack is a rich source of information, for example deleted files, fragments of the RAM or other data that may be reconstructed using file carving. [2]

The Art of File Carving

As explained above, file carving is a forensic procedure, used to reconstruct files. To get a little bit more technical, let us take a deeper look at forensic file carving and how it works.

Beforehand, let us assume that everyone by now knows what: 1) *A file system is*, 2) *a file is*. So, in a file system on a computer, lets take a Windows PC as a reference, a file is stored. Each file has an extension, indicating the type of the file, i.e. the content, and therefore how to handle it. An example would be a *Word Document* which would have either one of *.doc* or *.docx* as an extension, depending on the version of Microsoft Office used to create it.

The extension isn't always a reliable indicator to what a file is, it can be changed easily. Therefore, forensic examiners relay on the *Magic Number*. The Magic Number

is a unique identifier embedded within the file, showing us the real type of the file. An example here is a *JPEG* image; a JPEG image always starts with the hex-code *0xFFD8* and ends with *0xFFD9*.

Knowing this, and using a simple forensic tool, e.g. a hex editor, one can examine a file and determine its real type if there are any doubts, that the extension might be manipulated.

Back to file carving; there are many techniques for file carving, a few of them are listed below:

- **Header-to-Footer** - Recover files based on known headers and footers, or maximum file size.
- **File structure-based carving** - Recover files based on the internal layout, e.g. identifier strings.
- **Content-based carving** - Recover files based on the content of the file.

So considering the different file carving techniques and the magic number, a forensic examiner can use different tools to reconstruct possible evidence. Some tools used for file carving are: *Scalpel*, *FTK*, *Foremost*, and *Photorec*. Practical use of these tools is conducted during the exercise. [76]

Another important step in a forensic examination is the examination of metadata, which is explained below.

Metadata

Metadata is the most important artefact when it comes to digital forensics.

Metadata

Metadata is basically descriptive data about the actual data.

Metadata is a powerful source of information for a forensic examiner and can help solve a case. Metadata is basically data about data.

Metadata can reveal information about the data itself, data that was hidden or obscured or to correlate different data to a specific source. There are three types of metadata: File system metadata, digital image metadata and document metadata. Each of these store information about the saved data like MAC times, MAC standing short for Modified Accessed Created, size or author.

For all forensic examinations, the MAC times are of great importance.

Example: Bind, torture, kill

The serial killer Dennis Rader, known as the BTK killer, murdered 10 people in Kansas, USA, in the time between 1974 and 1991. BTK stands for bind, torture and kill, which was the way this serial killer followed during his killing spree.
In March 2004, the BTK killer sent a letter to the local newspaper *Wichita Eagle* to claim responsibility for the murder of a young mother in 1986. The newspaper contacted the FBI's Behavioural Analysis Unit (BAU) which in turn decided to communicate with the serial killer.
In January 2005 Rader left a note in which he announces, that the communication is going to be via a floppy disk. In February a purple floppy disk arrived at the television channel *KSAS-TV*. The disk contained a RTF file, short for Rich Text Format, named "Test A.rtf".
The analysis of the metadata of that file showed information like the creation and modification date as well as the title "Christ Lutheran Church" and the most important information being "Last saved by". In this section the name "Dennis" was recorded. With these traces, the BAU could initiate further steps that ultimately led to his arrest.
The BTK Killer was taken down with the help of digital forensics 30 years after he started killing. [46]

After a successful examination and analysis phase, which revealed inculpatory evidence and indicates a collaboration between Bob and Dave, it is time for the last phase. Grace and Frank need to document everything, e.g. all results and steps to clearly incriminate Bob and prove his involvement in the illegal selling of the hardware. [2]

4.7 Phase 4: Documentation

The last phase, probably the most important one in a forensic examination, is the documentation phase. During this phase, all steps taken, all results found, are documented and held within a single report.

This is important for a case which will be presented in a court of law, so a third party investigator can verify the findings. [2]

Grace and Frank took notes during the first three phases, which they will combine to a single report. The report usually contains the answer to the five questions: What, where, when, why, and who. Additionally, it is interesting to find out how a forensic incident happened and to mention what lessons can be learned for the future.

Next, the results of the forensic investigation conducted by Grace and Frank are presented.

4.7.1 Results

Grace and Frank have found incriminating evidence, that indicate a communication between Bob and Dave. Moreover, emails and cached websites were found, which prove Bob's intent, e.g. selling used hardware to earn extra money.

The reconstructed emails show a conversation between Bob and Dave, which includes a bargain about the price of the hardware.

Bob searched for suspicious keywords, i.e. price of used hardware, and the cached websites found by the investigators absolutely prove Bob's intent.

A deeper analysis of the operating system also revealed the presence of an external mass storage device, e.g. a USB thumb drive, to which files were transferred to. Due to the fact that Bob denies the presence of such a device, Grace and Frank can surely say that Bob is lying.

Following, the answer to the 5-W's, how, and lessons learned are presented.

5-W's, How, and Lessons Learned

To finally close this case, Grace and Frank finish their report by providing the answers to the questions important for a forensic examination. The answers are provided below:

- **What** - The first question to answer is what happened. Grace and Bob summarised the incident as following: *After an incitement of an employee, suggesting that a number of hard drives were missing, a forensic investigation was started to incriminate the suspected employee. The employee Bob, was suspected to have illegally sold hard drives to a third party which led to the publishing of secret government documents.*

- **Where** - An easier question to answer is where an incident happened. The investigators answered this question as following: *The forensic incident happened within the company of Alice, which is specialised in disposing of government used hardware. The main scene is the laboratory of the employee and primary suspect Bob.*

- **When** - Thanks to the information gathered from the metada, and with the use of forensic tooling, a comprehensive timeline was constructed. The investigators have summarised the events: *The first contact between Bob and Dave took place on the 18th of September of 2018. During a course of three weeks, Bob and Dave have exchanged multiple emails and different websites were visited that incriminate Bob.*

- **Why** - The answer to this question is usually not clear, but in our case, a testimony of the CEO Alice helped clear the air: *The CEO has testified that on*

the 15th of September of 2018, Bob has asked for a payraise. Alice has refused such a raise which ultimately led to Bob's actions.

- **Who** - Mostly, this question can not be answered, due to the lack of evidence. In our case, the clear suspect was and is Bob, Grace and Frank suggested that: *Due to the incriminating evidence found on the suspects computer, i.e. emails and cached websites, as well as the indication of a missing portable storage device, it is clear that Bob has sold the hard drives which led to the publishing of secret documents.*

In addition to the five questions answered above, it is interesting to find out how an incident happened. In our case, the unauthorised publishing of secret documents happened because hard drives that were sold by Bob, were not correctly shredded and data was reconstructed by a hacker, which was then published.

Lessons learned for Alice's company may include a better payment of employees to prevent rouge actions, and a dual control principle while shredding the data off the hard drives, to ensure correct shredding and to prevent the reconstruction of data.

Verification of Results

As a last step, the case is presented in a court of law, and the investigators Grace and Frank need to testify and prove the correctness of their results.

Optionally, e.g. if credibility of the report is questioned, results can be verified by a third party investigator and the authenticity of the data is verified using the original hashes. These hashes are then compared to the duplicated images, which ensures their compliance.

Using the report generated by Grace and Frank, any forensic investigator can track and reconstruct the examination and hopefully conclude the same results as our investigators.

The investigation is done, Bob was incriminated for illegally selling hardware that was supposed to be disposed of, which led to the publishing of secret documents.

Following, a quick summary of this chapter is provided.

4.8 Further Reading

This section will provide further reading material for specialising on specific topics in the context of Computer Forensics.

- **Forensic Analysis of BIOS Chips** - This paper provides a deeply practical guide to the forensic analysis of BIOS chips. Tips for forensic examiners as well as for anti-forensic enthusiast are provided.

- **Data Carving Techniques** - This free technical report from SANS provides the reader the required basics for the art of data carving.
- **Windows Registry Forensics** - This paper provides an insight of the power of the Windows registry and its importance to forensic examinations, focusing on incidents involving removable storage devices.

The next section is a summary of this chapter, providing a quick insight of all discussed topics.

4.9 Summary

A lot of information about computer forensics, with focus on computers using Windows as an operating system, has been introduced in this chapter. All the facts explained here are important for a forensic examiner, but more important though is the ability to practically use these facts and tools to run a forensic examination of a computer.

The phases of a forensic examination involving a computing device have been introduced and explained using our use case. Deep technical information about a few topics have been given, e.g. examination of BIOS chips and Windows Registry.

Some recapping of information already known to computer scientists was done, to make sure that all students are on the same level of knowledge.

All tools mentioned here and others will be practically used in the exercises, giving the student the opportunity to practice hands on.

The next chapter will focus on mobile forensics. The principles, especially forensic soundness, securing digital evidence, and the double verification principle are also applied in mobile forensic but will not be explained once again.

The focus will lay on techniques used during the forensic examination of mobile devices, what kind of challenges those devices create, and again this will be done using a fictional use case.

But firstly, and as a ritual for all chapters, below, a real case is provided, which was solved using computer forensics, specifically using metadata analysis.

4.10 Review Questions

1. Define Computer Forensics using your own words.
2. What steps are involved in a typical Computer Forensics investigation? Please consider both pre- and post-accident steps.
3. How are the different evidence sources classified? Come up with your own and compare them to the ones defined within the literature.

4. Give five example storage locations of latent data?
5. Bring in order; from most volatile to stable, following types of data:
   - Running Processes
   - Network Traffic
   - RAM
   - Floppy/Disk
   - Hard Disk
   - Network State
6. What does MAC in the context of digital forensics stand for? Give an example of what it is used for in an investigation.
7. What is File Carving? Which tools aid with that process and how do they work?
8. Is there an equivalent to the Windows Registry in OSX and Linux? If yes, please elaborate.
9. From a forensic point of view, why is NTFS favoured over FAT? What are the pros and cons of FAT in contrary to NTFS?
10. Explain the difference between BIOS and CMOS? What is the task of each of them, how are they separated and what do they have in common?

5 Mobile Forensics

In our second technical chapter, Mobile Forensics, we will take on the routines and techniques of a forensic examination in a mobile device scenario. The structure of this chapter is similar to the Computer Forensics chapter.

First of all, we will introduce two real life cases which were solved using Mobile Forensics as a kick off and motivation for this branch.

Following, our own definition of Mobile Forensics is presented, as well as some challenges specific to the Mobile Forensics branch of Digital Forensics.

As with Computer Forensics, during a forensic examination, a specific set of phases is always conducted. We will not explain the phases again, because they were already explained in the previous chapter, rather we will focus on what the differences are and what is important specifically for Mobile Forensics.

Like with the previous chapter, we will introduce our own case study, which will consist of a fictional forensic case involving mobile devices.

After the case study, we will break down the phases of the forensic examination, taking a closer look at the special techniques, steps, and hardware used during a forensic examination of a mobile phone.

A short summary will recap all information briefly and serve as an intro for the next chapter: Network Forensics.

Without further a due, the section Motivation is presented next.

5.1 Introduction

Computer Forensics, as mentioned in the previous chapter, is one of the most important branches of Digital Forensics, but it is important to remember, that Mobile Forensics is also as important.

One would ask, why is Mobile Forensics as important as Computer Forensics? Well, the answer is simple: taking the United States as a Reference; in 2015, 377.9 million wireless subscriber connection of smartphones and other mobile devices occurred [43]. As we can see from the statistics, mobile devices are wide-spread and in contrary to computers, are always on, have GPS, and accompany their users the whole day, no matter when, no matter where.

To better understand Mobile Forensics, one has to understand that mobile devices are more than just mobile phones, but rather they encompass a wide array of devices, ranging from tablets and GPS units, to PDA's and wearables, e.g. smart-watches.

These devices contain a lot of personal information, and for forensic examiners, these devices pose a literal gold mine of information.

Let us define in the next section, the term Mobile Forensics, and than introduce a few challenges that forensic examiners might face during a forensic examination of mobile devices.

5.1.1 Definition

As with Computer Forensics, nearly every book, article or forensic related agency, defines the different branches differently. In the end, all definitions present the same information, only a little different than the others.

Again, we took a few definitions of different sources and combined them to our own definition of Mobile Forensics.

Mobile Forensics

Mobile Forensics is the application of forensically sound techniques and principles, to gather electronic data off mobile devices for legal purposes or corporate ones. Mobile devices contain lots of personal information, therefore Mobile Forensics also describes the art of filtering relevant from irrelevant data considering the criminal or corporate case. [43] [36]

When comparing Mobile and Computer Forensics, one quickly realises which challenges might arise during the forensic examination of a mobile device. Well if not, the next section is helpful.

In the next section, we will mention and explain a few challenges that arise, specifically during a forensic examination of mobile devices.

5.1.2 Challenges

A few challenges arise when examining mobile devices. The nature of these challenges is inseparably connected to the fact that there are a massive amount of different types of mobile data, as well as applications running on those. Another reason is the different kinds of security mechanisms, which most computing devices, e.g. computers and laptops, do not have.

The connectivity to the cloud also plays and important role. A look at these challenges is given below.

Platforms

As mentioned before, what does one understand under mobile device? Smartphone? GPS? Tablet? Camera? Yes, all of the mentioned and many more count as mobile

devices.

We are purposefully not classifying laptops as mobile devices even though the are, because the forensic examination of laptops has a rather computer-like nature and not a mobile-like one.

Because of this vast amount of available platforms, a forensic examiner needs to be schooled in different types of devices, to successfully examine them.

Another reason that makes this challenge extremely hard to anticipate is the fact that the manufacturers change their concept quarterly, making it difficult for examiners to stay up to date.

Applications

The heart of mobile devices, specially mobile phones and tablets, are with no doubts the applications. There is an *app* for everything. It does not matter if it is social media, music and video streaming, or productivity apps.

Creating an app has never been so easy, which is one of the reasons why mobile applications are always far from secure. In Q1/2018, 3.8 million apps were available on the Google Play Store.

The fact that applications ask for permissions that they actually don't need, for example, a calculator app asking for permission to access contacts, makes a forensic examination even harder.

Cloud Data

As we all know, mobile devices are small, compact, and have limited storage and computing capacity. To overcome this burden, most mobile devices relay on cloud storage for backups.

The fact the nearly all smartphones are connected to the cloud, makes a forensic examination of all relevant files nearly impossible. It is not sufficient to seize and analyse the device only, but one has to recurs down the trail of cloud data, to make sure all relevant data gets examined.

Security Mechanisms

Another rather disturbing fact for forensic examiners in case of mobile devices is the vast amount of different security mechanisms that exist for these devices. Typically, computers have password protection, in some new devices, face recognition as well as finger print authentication are available.

Literally every modern day smartphone or tablet has at least four different security mechanisms, e.g. password, PIN, pattern, and *biometrical lock*. On top of that, must smartphones encrypt personal data with TPM modules, so there is no way of extracting the data without knowing the decryption keys. [71]

Biometrical Lock

A biometrical lock is a security mechanism relaying on a biometrical feature of the owner. A biometrical feature could be the face, a finger print, a voice sample or even in modern device the iris.

This makes the forensic examination of mobile devices such a difficult task. Now, let us take a loot at the actual forensic examination of these mobiles devices.

5.2 Forensic Examination of a Mobile Device

Although the forensic examination in general, no matter what kind of device it is, is always the same, some principles for Mobile Forensics need to be considered.

Mobile devices are mostly critical evidence, due to the amount of data they store. The data stored ranges from pictures and videos to GPS coordinates and connected hotspots. All these information are potential evidence, both inculpatory and exculpatory.

Following, we will take on the three important phases of a forensic examination of a mobile device: seizure, acquisition, and examination and analysis.

5.2.1 Seizure

Taking into consideration that most forensic investigations are of criminal nature, i.e. the presentation of the evidence in a court of law is required, it is important the all the phases, specifically the seizure phase, happens in a legally and forensically sound manner.

For the seizure phase it is important that a legal authority, e.g. police, is present before seizing any evidence. This is a kind of security policy which ensures that the seizing was done legally and cannot be refuted in a court of law, i.e. ensuring the double verification principle.

Important information like *IMEI* (International Mobile Equipment Identity) and *MEID* (Mobile Equipment Identifier) need to be documented, for them being the only way of uniquely identifying a mobile device, hence pinning it to its owner.

IMEI/MEID

IMEI, short for International Mobile Equipment Identity, and MEID, short for Mobile Equipment Identifier, are unique identifiers for mobile devices.

As with all forensic examination, also in Mobile Forensics, it is important to decide before hand what the goal of the investigation is, so a plausible reason for seizing a

certain mobile device is present.

Due to the fact that mobile devices usually accompany their owner the whole day, biometric evidence like fingerprints are left on them, so it is important to wear gloves, because not only digital evidence is of interest, but also good old physical evidence as well.

A forensic examiner should know that in case of mobile devices, the data can be stored in different places:

- On the phone
- On the SIM card
- On the memory card
- In the cloud
- In the cellular provider's records

As we see, more sources of data exist, if compared to Computer Forensics. A forensic examiner of mobile devices needs to be trained in handling SIM cards, a vast amount of different kinds of memory cards, and data which is stored in the cloud.

SIM Card

A SIM, Subscriber Identitiy Module, is an integrated circuit on a chip meant to securely store the International Mobile Subscriber Identity (IMSI) and other related cryptographic keys. SIM cards can also store contact information. All GSM and LTE capable phones operate and authenticate in the network using SIM cards.

Because of the fact the cellular provider's store information, a long legal process before getting the records of a smartphone is guaranteed.

The documentation of the incident scene is also important. All devices should be photographed before seizure, and a forensic examiner should always be present to ensure forensic soundness. [43]

Next, the acquisition phase of a mobile device forensic investigation is introduced.

5.2.2 Acquisition

The acquisition phase, or collection phase as it was called in Computer Forensics, is the phase were the forensic examiner is supposed to retrieve data off the seized evidence.

This phase can be divided into identification and extraction. Interesting is that, in most countries patterns, passwords, and PINs are usually protected by law, taking

the USA as an example, specifically by the fifth amendment. But biometrics on the other hand, even though being convenient for unlocking phones and tablets, are not protected by law and can therefore be used to unlock the devices against the will of the owner.

Data that is stored on a mobile device, is also mobile. The data is not only present on the device itself, but rather it leaves traces across the whole geographical fingerprint of their owner. So for a forensic examiner, identifying data that is synchronised across devices is crucial, because if data cannot be extracted directly off the phone, maybe it can be elsewhere.

A burden that all forensic examiners carry, specially the ones specialised on Mobile Forensics, is the ever-changing, non-stopping trend of mobile Applications. These applications grow in numbers and functionality, so it is of great importance to create a full list of all applications present, some of them might contain important back up data.

So, identifying the data which is important for later examination is not easy, but extracting them is not easy as well. Typical imagine like its used in Computer Forensics is not possible with most mobile devices, so a different way of extracting information is needed, here its called acquisition.

SIM card imaging is very important, and all Mobile Forensics examiners should know how to accomplish it. As with all forensic examinations, all analysis and manipulation is only done on replicas, and under no circumstance on the original set of evidence. [43]

Next, a closer look at the examination and analysis phase of a forensic examination of a mobile device is given.

5.2.3 Examination and Analysis

The examination and analysis phase is only to be conducted by specially trained examiners and no pre-examination by first responders, e.g. police officers, is to be allowed.

The evidence, securely stored for transport, is to be submitted to a forensic examiner, which will then be examiner by those, following the golden rules of a forensic examination, e.g. forensic soundness and so on.

It is important to understand that there are many different types of data found on a mobile device, which could possibly be important evidence. Some data that is found on a phone:

- Address book and call/SMS/MMS history
- Email and web browser history
- Photos and videos

- Music, documents and other files
- Social media information
- Application and deleted data

As mentioned a few times, if criminal or corporate investigation, a forensic examination is to be conducted as if it is to be presented in a court of law. Some rules apply on evidence to be admissible:

- Authentic
- Complete
- Reliable
- Believable

And those do not only comply to Mobile Forensics, but to all branches of Digital Forensics.

As with Computer Forensics, many tools aid the forensic examiner during this phase. All used tools need to be documented, all changes as well. In this phase, two approaches exist: Invasive and Non-Invasive methods. More to these methods will be presented in a later section.

Due to the vast amount of different types of mobile devices, no on-size-fits-all solution exists, so a sheer amount of different tools need to be available and trained for. [43]

Next, the fictional case study is presented, including all involved individuals and entities, as well as a look at the problems and goals of the forensic examination conducted is given.

5.3 Case Study

In this chapter, our case study is involves a forensic examination of a mobile phone as well as some evil neighbours that were trying to ruin the marriage of Bob and Alice.

Firstly, the scenario is explained, presenting all important information. Following, a view of all involved individuals is given. After that, a list of all important entities, e.g. evidence and its state, is provided. Lastly, a brief discussion of the problems and goals of the forensic examination is given.

5.3.1 Scenario

Bob and Alice are happily married and own a lot of real estate. They bought real estate during the financial crisis, and now they make profit selling some of the real estate at higher prices. Their neighbours Frank and Grace were proud owners of two coffee shops downtown, but during the financial crisis, they have lost both coffee shops and must now both work 60 hours per week, to keep up their lifestyle.

Both couples are good friends and usually do stuff together, stuff that neighbours usually do: grilling in the backyard, movie nights, and parties.

Since the financial crisis, Frank and Grace distanced themselves from Bob and Alice, because they are kind of mad that it didn't affect Bob and Alice as well. Due to the fact that Frank and Grace were close friends of Bob and Alice, they know that Bob and Alice agreed on a marriage contract stating that if they divorce, all real estates are transferred to a humanitarian agency, so that neither of them gets any of it.

Frank and Grace, being as evil as they are, searched the dark web for an evil hacker that might help them with a little scam, that might ultimately lead to a divorce of Bob and Alice. They found and hired Eve, a black market hacker.

Eve came up with an evil plan, to trick Alice into thinking that Bob is cheating on her. While Bob was at a coffee shop with open WiFi, Eve had hacked Bob's cellphone and gained remote access. She started spoofing chats between Bob and a fictional other woman, initiate calls at late night hours, and send the one or the other explicit photo to Bob.

Alice started getting suspicious and didn't believe Bob, which was desperately trying to state his innocence. Alice had her mind made up and wanted a divorce. Bob being sure he is being set up, hired a forensic examiner specialised on mobile device, to find traces of a possible hack on his phone, so he could prove his innocence to Alice.

Charlie, a well trained forensic examiner, specialised on mobile devices, and his trainee, seized Bob's phone, documented his immediate whereabouts before the begin of the hacks, and took note of the exact happenings.

Back at the laboratory, Charlie and his trainee identified and extracted all relevant data, securely stored the original evidence and started their forensic examination.

Following, a quick overview of all involved individuals is given.

5.3.2 Individuals

Individuals involved in the forensic case and their roles, are listed below:

- **Bob and Alice** - Married couple, real estate owners.
- **Bob** - Possible victim of a hack, or a cheating bastard.

- **Alice** - Disgruntled wife, wants a divorce.
- **Frank and Grace** - Bob's and Alice's neighbours, evil couple, trying to set up Bob out of envy.
- **Eve** - Shady black market hacker.
- **Charlie and Trainee** - Forensic examiners specialised on mobile devices.

All the individuals play an important role in this forensic examination. Following, all entities, i.e. digital evidence of interest, are listed below.

5.3.3 Entities

The primary and only digital evidence available is Bob's phone. The coffee shop with free WiFi which Bob visited, is also an important place of interest. Below, the technical specifications of Bob's phone:

- **State** - Powered on and unlocked.
- **Operating System** - Android Nougat.
- **Storage** - 64GB of storage consisting of 32GB of internal on-chip storage and 32GB of *mirco-SD* storage.
- **Connectivity** - WiFi, mobile data and GPS.

The investigators have full access to Bob's phone, obviously, because he granted them access to prove his innocence. The examiners contacted Bob's cellular provider and asked for his records. The examiners also visited the coffee shop and asked for a copy of the WiFi visitor log, consisting of MAC addresses of all users that were connected to the hotspot.

5.3.4 Problems and Goals

The main problem facing the examiners is the fact that they have to find exculpatory evidence, meaning, evidence that will exonerate Bob and prove his innocence.

On top of that, they have to go through the long never ending legal channels to get a hold of the cellular records of Bob. Thankfully, the coffee shop was in a cooperation mood, and handed over the visitor log of the WiFi without further fiasco.

As with all forensic examinations, the examiners have to seize, identify, collect, and examine all relevant data in a complete and correct manner to ensure acceptance of presented results.

In our case, there is no corporate or criminal investigation, but rather a personally requested investigations, so the examiners also have to tread carefully to not expose irrelevant information of Bob.

The goal of this investigation as said before is to prove that Bob is not cheating on his wife Alice. Primarily, it is of interest to find prove of a possible hack, so that Bob's statement gets more believable.

Secondary goal would be to find the hacker and maybe understand his or her intentions.

Next, we will accompany Charlie and his trainer through the forensic examination, and we will start with the seizure phase.

5.4 Seizure

During the seizure phase in a Mobile Forensics scenario, it is important to remember that mobile device have different interfaces connectivity, e.g. WiFi, mobile data, bluetooth, GPS, NFC, and infra-red.

So Chalie and his trainer have to consider all possible interfaces, and to ensure no further alteration of Bob's phone, they have to securely transport the evidence.

Below some techniques and methods used specifically in case of Mobile Forensics.

5.4.1 Airplane Mode

To prevent further remote manipulation of the data on Bob's phone, or to prevent incoming or outgoing connections, the examiners put the mobile device in *Airplane Mode*. As the name suggests, this mode is meant to be used while in an airplane, to prevent interference with the airplane electronics.

This mode comes in handy, and is basically available on all mobile devices. So for a forensic examination of a mobile device, network isolation is always initiated and should be done as soon as the evidence is seized.

5.4.2 Phone Jammer

Another tactic used by police or incident response teams is the use of *Jammers*. Jammers are to be used under strict regulations and cannot be used by private persons, to prevent miss use and possible interference with important networks.

The jammer jams any incoming and outgoing calls and messages, and with that disabling a phones connectivity, if there is no way of setting the phone in airplane mode, maybe due the phone being locked.

5.4.3 Faraday Bag

A more subtle way of isolating a mobile device, if jammer and airplane mode are not an option, is to use physics. Yes, physics! The use of a *Faraday Bag* ensures complete isolation of a device and prevents all connections from and to the outside world.

Typically, the faraday bag is hooked up to a power source to prevent the phone from shutting down, in case that the unlock keys are not available. Also, the *Stay Awake* function of mobile phones is usually activated to prevent them from going into sleep mode. [43]

Charlie and his trainee, bagged up Bob's phone properly, they have access to the phone so they put it in airplane mode, and just to be sure they bagged it up in a faraday bag and hooked it up with an external battery pack so it does not shutdown, so they can analyse volatile data as well.

Coming up next, the acquisition phase of our forensic examination.

5.5 Acquisition

Our forensic examiners successfully seized all evidence and are back at their laboratory. Now they have to identify important digital evidence and extract them off the phone.

With mobile devices it is not always as trivial as with computing devices, simple imagine is not an option.

During this section, we will explain the difference between *physical acquisition* and *logical acquisition*.

After that, we will list the types of data that might exist on a mobile phone, cross referencing their importance to the forensic examination in general.

5.5.1 Identification and Extraction

As mentioned before, the acquisition phase in Mobile Forensics can be divided into two sub-phases: identification and extraction.

During the identification sub-phase, Charlie and his trainee try to identify the digital evidence, i.e. classify it, so they can prepare the right tools and the needed hardware for later examination. The create a list of all apps installed on Bob's phone to verify their integrity and to check them for possible information related to the case.

Bob's phone is synchronised with his PC, so whenever he enters the WiFi in his home, a backup is made and stored in a network attached storage device. Charlie and his trainee need to consider this during their examination.

As soon as they identify all related digital evidence, they can start with the extraction of the information using the tools they prepared.

Now, let us take a loot at the difference between physical and logical acquisition.

Physical Acquisition

During physical acquisition, a physical memory dump is initiated. The method captures all the data from the flash memory, including the remains of delete data still present on that memory. [36]

The data is in raw format, basically, zeros and ones. Methods to convert this data into human readable data are applied by Charlie and his trainee.

Logical Acquisition

Logical acquisition only extracts files and folders, e.g. the structure of the file system present on the flash memory, not including any deleted data. [36]

Usually, tools are used to make copies of pictures, call history, and other possible important information. Charlie and his trainee use an adequate tool and create a logical copy of all contents, while the physical copy is progressing.

There are different types of data present on a mobile device. Mobile phones for instance, are a gold mine and contain lots of personal information of their owner, the immediate vicinity, and previously visited locations.

Let us take a look at the different types of data available, and state their importance to a forensic examination.

5.5.2 Types of Data

Mobile devices accompany us on our way to work, to vacations, to doctor appointments and even to bed. Due to the high connectivity of mobile devices through a vast amount of interfaces, important information is stored in them.

Call Detail Records

CDRs, or Call Detail Records, represent information stored by service providers which is used to improve network performance.

Although being inaccessible without a long lasting legal process, the CDR contains useful information to a forensic examination:

- Call start/end time
- Originating and terminating towers
- Whether a call was outgoing or incoming
- Call time duration

- Caller and called person

So for Charlie and his trainee, which have already asked for a copy of the CDR from the cellular provider, the CDR may contain bulletproof evidence of Bob's innocence.

Global Positioning System

For a forensic examination, imperial evidence, i.e. evidence that can be measured and put into relativity, is the best kind of evidence.

GPS (Global Positioning System) provides the examiner with such imperial evidence. Information like the suspects whereabouts at the time of crime can be extracted through GPS information.

Charlie and his trainee can now prove that Bob was at the coffee shop during the time he has stated.

Example: 65-year-old Hitchhiker Found Dead in Ontario

In the Canadian online magazine Quartz on the second of November of 2016, an article about a 65-year-old hitchhiker found dead was posted.
A year before, a 65-year-old hitchhiker was found dead, and after a year of investigations with no leads, Canadian authorities switched from old fashioned police work to digital forensics.
The body of the hitchhiker was found partially burned, dead, near the town of Erin in Ontario. Just a day before he was found dead, Frederick John Hatch, the hitchhiker, was seen alive, nearly 300 miles away in Nepean, Ontario. It was a mystery how he had covered this much of a distance.
Ontario Provincial Police have received a court order allowing them them to identify the mobile phones that were in the immediate vicinity, which were around 7500 phones, between the times of interest.
The police then sent two text messages to all cellphone numbers, one in English and one in French, asking the people to help identify possible leads or suspects to solve this case.
In a later press release, the police have assured that they are only using the phone numbers, no other information like names are being stored.
A 50.000$ reward was promised to anyone who provides details that lead to the arrest and conviction of the murderer.
Again, mobile forensic helped, specifically the forensic analysis of geolocation-data has played a role in normal police work, not yet solving the case, but at least a promising new step. [6]

Application Data

Most apps have access to the internal storage of a mobile device and can therefor store important information.

With that said, forensic examiners should always check for installed apps and document what kind of permission they have, so they can identify what kind of data the apps could and are storing.

Short Messaging Service

Even though being old fashioned and outdated by online messaging services, Short Messaging Service or SMS, is a widely used way of communication.

These messages leave a trial of evidence like data and time of the message, and the phone number of both receiver and sender.

Information like that can be crucial in a court of law and actions can be pinpointed to a single person.

Charlie and his trainee consider all messaged Bob has sent, but the fact they carry his phone number does not help him, but rather it incriminates him.

Example: Two 13-year-old Andover Girls Missing

As stated in the StarTribune on the 6th of October in 2014, two 13-year-old girls from Andover in Minnesota went missing.
Commander Paul Sommer has spoken to the press and confirmed that the girls were found within 24 hours, and not by a search-and-rescue unit, nor by a K9-Unit, but rather by an officer sitting in a forensic lab.
The forensic examiners seized and analysed the girl's iPods and smartphones. Quickly, and with the help of established forensic methods and tools, evidence of the whereabouts of the girls were found.
Ultimately, the girls have been found in a basement of a Burnsville man named Casey Lee Chinn, who was charged with felony criminal sexual conduct, kidnapping and solicitation of a child.
The parents reported the girls missing on 9:36 p.m. Monday. Detective Pat O'Hara has searched the girls room and found their iPod. A quick examination of the device has revealed sexually explicit texts ranging two weeks back.
The originating geographic position of the sender of these texts was then triangulated and by next morning, the police were on scene searching the suspects house, where the girls were then found. [51]

Photo and Video as Evidence

Case closing evidence are photos and videos. If proven to be relevant for the investigation, and their authenticity is undoubted, photos and videos can be a tremendous

help during an investigation.

Photos and videos also carry geographic footprints, i.e. information about where the picture/video was taken, as well as an ID of the aperture that shot the picture/video. [43][36]

The examiners extract the explicit videos and photos Bob has received from the mysterious mistress, and analyse them, focusing on the metadata using a tool called *Exiftool*.

Now that Charlie and his trainee have identified and extracted all relevant data from Bob's phone, and a deep understanding of the different types of data present on a mobile device and their importance is present, we move on to the next phase.

Following, the examination and analysis phase of the forensic examination is given.

5.6 Examination and Analysis

The main difference between Computer and Mobile Forensics lays within the examination and analysis phase. Different methods are applied, considering the difference in the hardware examined.

The techniques used during the forensic examination of a mobile device can be categorised into two groups: *Non-Invasive* and *Invasive* methods.

Both groups contain various methods of analysing and examining data on mobile devices. A closer look at both methods is given below.

5.6.1 Non-Invasive Forensics vs. Invasive Forensics

Non-invasive, meaning less aggressive than invasive, are forensic examination methods used to analyse data without damaging the integrity of the evidence.

Invasive methods as the name suggests, might render the evidence useless and are only applied as a matter of last resort.

Usually, a forensic examination of a mobile device is started off with non-invasive methods. Charlie and his trainee need to be careful, some security mechanisms might wipe the device if a wrong password is entered too many times.

If no examination is possible due to severe damage to the physical condition of the mobile device, the forensic examiner should consider invasive methods. [43][36]

5.6.2 Non-Invasive Forensics

Non-invasive methods can only be applied if the evidence has not suffered severe physical damage. [43][36]

A few non-invasive methods are introduced below.

Manual Extraction

During *manual extraction*, the examiner analyses the mobile device by simple browsing it. The examiner uses the human input interfaces like touchscreen and keypad to access photos, videos, call history, and other.

The goal here is to look for eye catching evidence like incriminating photos or phone calls. There are tools to aid an examiner during this phase, but no extraction of deleted data is possible.

Logical Extraction

Logical extraction requires a fully equipped forensic workstation. The mobile device is connected to the workstation using one of the many available interfaces, e.g. Bluetooth, USB, etc..

The workstation is then used to send commands to the mobile device, requesting data, which the device then returns to the workstation.

This technique is simple and does not need much training, most forensic tools implement logical extraction.

Although being easy, logical extraction might indeed alter data or even add data to the evidence, and deleted data cannot be accessed as well. [43]

Joint Test Access Group Method

The *JTAG* method, is a non-invasive form of physical acquisition. If the device was damaged, locked or encrypted in a way that hinders software based extraction, JTAG might be the answer.

A so called Test Access Port (TAP) is accessed, instructing the processor to return raw data that is stored to its connected memory chips.

This method is designed for mobile phones, because mobile phone manufacturers usually provide the TAP interface to enable a low-lever interface independent from the operating system.

This method is labor-intensive, time consuming, and needs a lot of training. But it is worth the time, for it being a method of accessing data on a devices memory without jeopardising the integrity. [43]

JTAG - Defeating Android with a little Magic Box

For this being a technical chapter, let us dive deeper in to the art of using JTAG to defeat possible security mechanisms of an Android smartphone.

So, first of all, let us state that *TAPs* (Test Access Ports) are not available on iPhones, so this method is only valid for almost all android phones, which make up the great majority of the market anyway. JTAG is usually used when a phone is

locked, e.g. by a pattern, or is damaged, e.g. *bricked*, and cannot be accessed in any other way.

There is no ultimate guide, and this method is going to differ from phone to phone. Following, a simple yet general guide on how to extract a physical image of a device using the JTAG method:

- **Step 1** - Strip the phone down till the *PCB* (Printed Circuit Board) is visible. Identify the TAPs by researching for the specific device and its documentation. If no TAPs are visible, manual probing to pinpoint connector pins which are appropriate is done.
- **Step 2** - Some soldering work is needed to solder the wires to the right connector pins. The use of a solderless jig is also possible.
- **Step 3** - Connect the soldered wires to an appropriate, i.e. supporting, JTAG emulator.
- **Step 4** - With the software provided, read the flash memory after selecting an appropriate device profile. If non exist, manually configure processor/memory settings.
- **Step 5** - Proceed to analyse the extract physical image with standard forensic tools, to look for possible evidence.

It is also important to mention that the JTAG method can be also applied on network devices, tablets, and video game consoles. The sole requirement is a supported processor and working TAPs. Some companies provide JTAG extraction services, which usually take from three to seven days. [8]

Hex Dump

Hex dump as already mentioned in the Computer Forensics chapter, is a form a physical extraction of raw information which needs parsing to a human readable form.

The mobile device is connected to the workstation and a custom *Bootloader* is applied, so instructions to initiate a dump can be carried out.

The data that is extracted is in raw form, and a well trained examiner is needed to analyse it. With this method, deleted data can be accessed and analysed, optimally, file carving can be applied to reconstruct delete files. [43]

Following, a review of invasive forensic methods is given.

5.6.3 Invasive Forensics

Usually, invasive forensic methods tend to be more difficult and complex, hence requiring a well trained forensic examiner.

Invasive forensics is used when the device is damaged in a way that does not allow software based data collection, which leads to a more aggressive way of data collection, namely physical.

Chip-Off

With the *chip-off* method, a forensic examiner is able to collect data straight off the physical memory chip. The memory chip is basically removed from the damaged mobile device, and implanted in a functional device, allowing the extraction of information.

This method is very expansive and needs thoroughly trained examiners. The vast variety of chips makes creating a standard procedure difficult. Lots of hardware is needed to conduct this operation, e.g. soldering iron.

The information retrieved are on top of that in raw format, so standalone bits and bytes which need translation first. Any mistakes during this procedure renders the chip, which is also the only source of evidence, unusable.

It is recommended to use this method as a matter of last resort and only of the investigation has already tried out all other methods unsuccessfully, or if it is a matter of national security. [43]

Chip Off - The *Wary-Invasive* Forensics Method

As mentioned above, chip-off is an invasive forensics method which is usually only used when all other methods, including JTAG, did not, or cannot, work. As with JTAG, let us take a loot at the general steps of a chip-off procedure:

- **Step 1** - The memory chip of the mobile device has to be physically removed from its housing. To accomplish that, appropriate *heat*, i.e. de-soldering, and *chemicals*, i.e. adhesive removal, methods and tools are applied.
- **Step 2** After successful removal, the memory chip is cleaned at repaired of necessary.
- **Step 3** - With the use of chip programmers and available adapters, a raw image of the data is acquired.
- **Step 4** - The raw image is then parsed and analysed using standard forensic methods and tools.

Chip-off procedures usually take longer if outsourced and can range from five to ten days. In contrast to JTAG, nearly every device using *flash memory*, e.g. NAND, NOR, OneNAND or eMMC, are supported. This method has proved its practicality by extracting data off GPS units, USB drives, and vehicle components. [7]

Micro Read

Micro read is the most complex, expensive, and labor-intensive forensic method there is. A forensic examiner will examine the memory chip through an electron microscope to analyse the state of the physical gates on this chip.

That way, data can be seen in its most basic and raw form, which in return needs interpretation, meaning that the physical state of the gates is translated in zeros and ones to discover which ASCII codes are represented.

Therefore, micro read is also reserved for security critical cases and is rarely conducted during normal investigations. Following, a quick summary of this chapter. [43] [36]

Due to the fact that full access to the phone is present, and the phone is not damaged in any way, Charlie and his trainee can apply non-invasive methods to find possible exculpatory evidence.

The examiners apply manual and logical extraction, as well as metadata analysis on their workstation. The evidence they examine are the text messages and pictures that Bob has received.

Taking a closer look at the text messages, they realise that the text messages Bob has allegedly sent, originated at location x, while Bob's geographical location at the time was location y. So, the text messaged were not sent by Bob. This is underlined by the CDR, which proves that Bob's phone with its unique IMEI, did not send any text messages at the interested time.

Now to the pictures: the pictures were all downloaded from the internet, which can be seen while analysing the metadata of these files. This is also an indication for Bob's innocence.

A further examination of the phone showed traces of a remote access software, that was installed on Bob's phone. With this remote access software, an indication of a possible hack is present.

The analysis of the WiFi visitor logs at the coffee shop proves, that Bob's phone (MAC address) was present. The examiner quickly realise that the source of the infection must of been the coffee shop, which usually provide free WiFi and have very few security mechanisms.

Following, the examiners present all the results they have found to Bob and Alice, hoping to prove Bob's innocence.

5.7 Results

After the forensic examination of all relevant evidence, Charlie and his trainee have found following exculpatory evidence:

- *Spoofed text messages*, originating at a tower different to the one Bob's phone was connected to.
- *Pictures downloaded from the internet*, and not actually belonging to the woman Bob supposedly cheated on Alice with.
- *Bob's presence at the coffee shop* was proved due to the visitor log.
- *CDR information* from the cellular providers underline the spoofed text messages.
- Traces of a *remote access software* on Bob's phone were found.

These evidence prove Bob's innocence and changed Alice's mind, which made her back off from her decision to file a divorce.

The examiners consulted a government agency handling forensic cases and provided them a sample of the remote access software. The agency quickly found a match between the signature of the software and some previous cases and apprehended the suspect, Eve.

The prosecution offered Eve a deal, in return she gave up her employers, Frank and Grace, which were then prosecuted and convicted of committing cyber criminality with the intent of sabotaging a marriage.

5.8 Further Reading

As with the previous chapter, this section will provide further reading material relevant to the topic Mobile Forensics.

- **The Role of Mobile Forensics in Terrorism Investigations** - This paper demonstrates how Mobile Forensics can be deployed to uncover important evidence in criminal acts of terror.
- **Forensics Data Acquisition Methods for Mobile Phones** - In this paper, the authors provide a comparison of modern Mobile Forensic data acquisition techniques and an analysis of their efficiency and effectiveness.
- **An Analysis of Smartphones Using Open Source Tools vs Proprietary Tool Cellebrite UFED Touch** - The thesis is a direct comparison of the closed source tool Cellebrite used by government agencies for Mobile Forensics, and alternative open source tools.

5.9 Summary

As we see from the fictional case study, and from the provided real cases, forensics help solve cases, criminal, corporate and private ones.

During this chapter we explained Mobile forensics, providing a definition, and a few challenges that arise during forensic examinations of mobile devices.

Our case study involved an innocent Bob that was framed by his envious neighbours, but his innocence, thanks to the examiner Charlie and his trainee, was proved. Analysing the mobile phone of Bob revealed exculpatory evidence and provided leads to the actual perpetrator.

Mobile Forensics is an important branch of Digital Forensics, due to the huge amount of mobile devices the are spread around the world. Mobile devices include cellphones, GPS, cameras, and other devices. Because of the high variety in platforms, Mobile Forensics examiners need to be trained well and have skill sets in different tools and platforms.

The phases of the a forensic examination of a mobile device were introduced once again, although focusing on the difference to computing devices. Tactics like the activation of airplane mode, the use of faraday bags for evidence transportation, and invasive and non-invasive forensic methods were introduced.

Charlie and his trainee, our forensic examiners, present the results and the evidences they found, which clear Bob of any wrong-doing.

5.10 Review Questions

1. What are, in contrary to Computer Forensics, specific challenges within Mobile Forensics investigations?
2. Two types of approaches were defined for Mobile Forensic investigations: invasive and non-invasive. Elaborate both. Take a specific method of one approach and explain it in detail.
3. What are CDRs? Look for official definitions provided by telecommunication providers.
4. In a Mobile Forensic investigation, different tools for digital evidence preservation are used. Name two of these and explain their task.
5. Define Mobile Forensics using your own words.
6. Explain the difference between logical and physical data acquisition in the context of Mobile Forensics.
7. Give five examples of data that resides on a mobile device which are specifically interesting for a forensic examiner.

8. Research following topic: On-Site Triage Processing. How does it fit within Mobile Forensics? What is it used for?

9. Cross referencing Mobile Forensics and Anti-Forensics: what is a plausible countermeasure for jammers? Hint: Modulation techniques.

10. Different phones, different platforms. Please collect statistics on the usage of the different mobile device operating systems. Reference your source and explain why you think the statistics look the way they do.

6 Network Forensics

The last technical chapter of this lecture will deal with the topic Network Forensics. Unlike Computer and Mobile Forensics, Network Forensics crystallises itself as a challenging task with lots of difficulties spread across the investigation process. An introduction to the topic will be provided consisting of a definition as with previous chapters and an overview of the possible challenges that face an investigator. Furthermore, due to the motto of Network Forensics: An ounce of prevention is worth a pound of detection, we will make a detour and explain the different prevention and detection techniques found within networking, e.g. Intrusion Detection, Intrusion Prevention, and Firewalls. Previous chapters have shown the different steps of a forensic examination, which usually consisted of the same terminology and were basically named alike. In Network Forensics, a special type of methodology is used during an investigation which is called OSCAR, which will be explained further along. When talking about networking, the ISO/OSI layers come to mind and seem inseparable. Even though the layers of networking are set as a pre-knowledge, a cross reference with Network Forensics is made within this chapter. We will look at the traffic protocols and network layers that are especially interesting for a forensic examination. Different strategies are followed by examiners during a Network Forensic examination, considering the data collection. Stop, Look, and Listen as well as the Catch-it-as-you-can techniques will be explained. Pros and contras are listed to help determine which technique is appropriate for which situation. Finally, a toolset for Network Forensics are listed and their capabilities and boundaries are considered. A correlation to network-based attacks is made to clarify which tools are appropriate.

6.1 Introduction

Network Forensics is to be considered the gold discipline of forensics in general. Unlike Computer and Mobile Forensics, Network Forensics is a fairly new discipline still in the making and lots of theoretical literature is being provided to enhance the process of Network Forensics. It is important to understand that all computers, mobile phones, even cars nowadays, are interconnected, most likely through a networking construct. This is what makes this discipline so fantastic and difficult: data is wide spread, and it is not in one place, but everywhere and nowhere. This makes it especially hard for investigators to collect all relevant pieces of evidence, or even determine relevant from non-relevant. Let us talk numbers for a second: according

to Statista, in the year 2015 we had a total of 15.41 Billion Internet of Things devices that were connected. Our current year almost doubles this to a total of 26.66 Billion only in the first quartal. A staggering 75.44 Billion devices are predicted to be connected by 2025. This is only considering IoT devices, now face the fact that there are at least exactly as much in form of computers, mobile phones, GPS devices, and soon cars. Now that we have clarified how much importance is behind Network Forensics, let us take a look at the definition of the term.

6.1.1 Definition

We will provide a definition which was thorough thought of and represents a precise definition which is based on many other ones.

Network Forensics

Network Forensics is the art of capturing, recording, and analysis of network packets to determine the source of a breach or attack against private corporations or government institutions. It is the discipline of gathering data from interconnected devices to pinpoint a crime to a single perpetrator. [55]

Next, an overview of the challenges of a Network Forensic examination is provided.

6.1.2 Challenges

As mentioned before, Network Forensics turns out to be a challenging task. Let us list a few challenges and clarify why in comparison to other types of forensics, Network Forensics is specially challenging [23].

- **Network data is changing constantly** - Network data, e.g. packets, connections, and protocols are changing constantly and fast. These types of data are viable for a forensic investigation and make it especially challenging to collect.
- **Pinpointing direct location problematic** - The determination of the exact originating point of network data, i.e. evidence, is problematic. Network devices are interconnected, and it is difficult tracing the originating sources.
- **Physical access difficult** - The physical access to network devices is often need, which turns out to be difficult most of the times, because network devices are scattered around and are not to be found in one location.
- **No persistent data** - In network device, e.g. routers, switches, persistent data is not wide spread. Most of these devices have volatile memory, i.e. after power loss comes complete data loss.

- **Investigation overhead** - The scanning of network segments within a forensic investigation causes different degrees of overhead. This is problematic, causing slower connections within corporation networks which interferes with normal procedures.

- **Legal aspect** - The legal aspect within a Network Forensics investigation are mostly unclear. It is difficult deciding which networks segments to scan and which are irrelevant for an investigation, and with each segment comes different legal issues.

As we see, in contrary to Mobile and Computer Forensics, Network Forensics deal with dynamic data which turns out to be not only an overhead but also a legal issue. After the listing of different challenges of Network Forensics, let us focus on the different prevention and detection techniques that are used to protect and monitor networks.

6.2 Prevention and Detection

As the motto of Network Forensics, it is important to prevent as much damage as possible, because prevention may be more difficult to setup, but is easier to cope with once configured correctly, while detection being easy, once a detection is made it is mostly too late. We will look at different prevention and detection techniques currently available [23] [18].

Intrusion Detection System

Intrusion Detection System, short IDS, is a system which monitors network traffic and activity searching for suspicious signs, issues, and alerts. Most IDS systems are only meant as an anomaly detection, but some can take actions against detected anomalous behaviour. Therefore, IDS systems are classified as a detection technique.

Intrusion Prevention System

Intrusion Prevention System, short IPS, are much like IDSs, although instead of monitoring passively for anomalous behaviour, e.g. malicious traffic, they actively block such packets by dropping them or denying rerouting. An IPS is a technique for prevention.

Honeypots

Honeypots are decoys, which represent systems purposely weakened, to lure an attacker into attacking that specific system. The Honeypot is setup to then detect such attacks and hacking attempts, and to gather information about the attacker and to notify respective administrators. The Honeypot represents a technique for detection.

Firewalls

The classic prevention technique in computer and network specially are firewalls. Firewall rules are defined which allow or deny certain services from accessing certain network ports. Firewalls are typically classified as prevention systems, but also function as a detection mechanism warning the user when such a breach is registered.

After the listing of different techniques used to prevent and detect network-based breaches, let us dive into the practical part of a Network Forensics examination. The OSCAR methodology will be explained in the following section.

6.3 Steps of an Investigation

In previous chapters, we defined the steps of a typical forensic examination. These were defined for Computer and Mobile Forensics and can be applied as is to Network Forensics. But to the state-of-the-art mentions following methodology for Network Forensics: OSCAR. The OSCAR methodology is used especially for Network Forensic investigations and consist of the following steps [18]:

6.3.1 O for Obtain information

The first step includes the creation of an incident description. This is followed by gathering data that is relevant for the incident discovery, which might include known persons involved, systems and data involved. Furthermore, it is important to document measures and actions taken by an organization or agency since discovery of an incident to establish a correct time line. Potential legal issues and goal of the investigation need to be defined.

6.3.2 S for Strategise

The forensic examiners need to gather and understand the goal set previously and the time frame of the forensic examination. It is important to organise and list resources.

The documentation and identification of evidence sources as well as an estimation of their value is to be given. The planning of the investigation in general is to be conducted during this step.

6.3.3 C for Collect evidence

This phase consists mostly of documentation. All steps within the collection of evidence are to be documented, evidence is to be lawfully captured, forensically sound and verifiable copies are to be made. A secure storage of all collected evidence is to be established, as well as a chain of custody. Later, the analysis of the made copies is to be conducted with the aid of legal tools.

6.3.4 A for Analyse

This phase aims to show a correlation between multiple sources of evidence, to establish a well-defined timeline and to highlight relevant incidents. It is important to corroborate all evidences gathered, to reevaluate the plan of investigation made in previous steps and to make interpretations. The investigator must build a working theory and is obligated to separate between interpretations and facts while documenting and presenting the outcomes.

6.3.5 R for Report

The final artefact is an understandable, complete, defensible, and most notably a factual report. This report is the centre of the investigation and the main outcome which is used within a court of law.

This methodology is cropped to fit a forensic examination in terms of network devices and is primarily used by incident response teams. Previously mentioned steps are still valid, but the OSCAR methodology specifies a well-suited strategy for Network Forensics. After understanding the steps of an investigation, it is time to introduce the different types of artefacts, i.e. evidence, that is interesting for a Network Forensic examination, and to specify their source. Therefore, in the following section we will present the ISO/ISO layers and their correlation to Network Forensics.

6.4 Network Forensics and the ISO/ISO Layers

As all of you know, the ISO/ISO layers represent the typical network stack and all computer scientists are required to have a basic understanding of these layers. For this being an advanced lecture with the master programme, we will not explain the layers but rather correlate them to possible forensic evidence. For starters, let us recap the layers:

- **Layer 1** - Physical
- **Layer 2** - Data-Link
- **Layer 3** - Network
- **Layer 4** - Transport
- **Layer 5** - Session
- **Layer 6** - Presentation
- **Layer 7** - Application
- **Layer 8** - Human (unofficial)

Now that the ISO/OSI layers were listed, let us correlate each layer to the possible artefact or evidence that might originate there [23].

- **Physical and Data-Link Layer** - Attackers might eavesdrop on bit streams of the Ethernet layer. Tools exist that monitor or sniff the Ethernet layer such as Wireshark. This requires a lot of storage, for the data being stored is in raw format and without context.
- **Transport and Network Layer** - For a forensic examiner, the examination of the network and transport layer are crucial. These include the inspection of routers and corresponding routing tables, authentication logs, and others. Reverse routing is used to determine source of corrupt packets.
- **Network Traffic** - A forensic examiner must examine the network services running on device such as WWW, email and chat clients. Server logs can be consulted to identify interesting services. Web servers and emails servers are very important and hide lots of data. They collect browsing history, email accounts, etc., all of which are interesting evidence sources.
- **Wireless Medium** - Not only wired but also wireless traffic must be collected and analysed. Smartphones and other devices usually communicate of wireless protocols. These devices contain voice communication logs. GPS data is also useful for pinpointing locations of perpetrators.

As we see, the ISO/OSI layer plays an important role in Network Forensics, and it is important that all examiners have a deep understanding of basic computer networking and distributed systems. Following, the two different data collection strategies within Network Forensic investigations are defined and explained, focusing on use case and pros/contras comparison.

6.5 Data Collection Strategies

Within Network Forensics, two different data collection strategies are established. The two strategies focus on different use cases and are therefore better suited for different tasks. Both strategies happen to have pros and contras which will be explained next [55].

6.5.1 Stop, Look, and Listen

The Stop, Look, and Listen strategy focuses on a delicate, goal oriented, approach of data collection. The data that is stored is data that is needed. Unnecessary data is filtered out and ignored. These filters must be written and agreed upon beforehand. The creation of strong and correct filters is a non-trivial task is in its preparation a time-consuming task. The analysis of the data happens in real time. One major positive aspect is the amount of storage needed. The storage needed is limited and does not reach unrealistic dimensions. The main setback is the high amount of CPU performance needed for real-time filtering and analysing of tunnelled data.

6.5.2 Catch-it-as-you-can

Unlike the previous strategy, the Catch-it-as-you-can method tunnels all data, relevant or non-relevant through a bottleneck and stores it all. This way, no previous preparation is needed, and a forensic examination can start instantly. It is important to consider the legal aspect of this method. The analysis and examination happen post-mortem and do not require as much CPU performance as the previous method. However, an exhaustive data set is guaranteed, and a full forensic investigation is possible due to the complete amount of evidence. Disregarding the privacy concerns, another setback is the large amount of storage needed for all the data stored.

Each strategy is suited for a different use case, for example the main difference is that Stop, Look, and Listen is used for live-forensics whereas Catch-it-as-you-can is rather used for a post-mortem approach of forensics. The coming last chapter will deal with the tools that are used for Network Forensic examinations and will describe their capabilities. Network-based attacks are considered and explained briefly.

6.6 Network Forensics Tools and Network-based attacks

The repertoire of Network Forensic tools is major. A lot of different, forensically sound tools exist and range from general purpose tools to tools for specific tasks [23]. Following, a list of tools sorted by purpose and a brief explanation is given:

6.6.1 Tools and Capabilities

- **General purpose tools — Packet collectors and protocol analysers**
  - dumpcap, pcapdump, and netsniff-ng: Packet sniffers
  - tcpdump, Wireshark, and nstat: Protocol analysers, used to inspect and record traffic. Both session- and packet-centric approaches supported.
  - Xplico and NetworkMiner: Network Forensic Analysis Tools (NFAT). Data-centric tools for traffic analysis
- **Specific tasks tools — Task-oriented programs and tools**
  - snort, suricata, and bro: Intrusion detection
  - ngrep: Regular expression matching
  - nfex and driftnet: file and picture extraction
  - dsniff, firesheep, ettercap, creds: Sniff passwords or HTTP sessions
  - mailsnarf and smtpcat: Email extraction
  - ntop, tcpstat, tstat: Network statistics
  - ssldump: Extract SSL information
  - tcpflow and tcpick: Reconstruct TCP flows
  - pOf and prads: Fingerprinting

As we see, the different tools achieve different tasks and have different capabilities, for example network traffic capturing, analysis, evaluation, detection of anomalies, aggregation, and security relevant investigations.

6.6.2 Network-based Attacks

Most forensic incidents related to networks, are network-based attacks and intrusions. To get an understanding of how the tools help the investigators, it is important to mention what kind of network-based attacks exist. Following, a list of network-based attacks.

- **Man-in-the-Middle** - M-i-t-M attacks are complicated and require deep knowledge of networking as well as appropriate tooling. This kind of attack represents a third, malicious party that sniffs and records packets being sent from one node to another. This malicious party can alter, store, or drop packets.
- **Ping Flood** - Ping Flood is a simple Denial of Service (DoS) attack, where a malicious third party overwhelms a victim with ping packets.

- **Buffer Overflow** - These attacks require advanced coding skills and misuse weak programs to cause an overflow in the data structures which could lead to failure of procedures or to privilege escalation.
- **SQL Injection** - As with Buffer Overflow, SQL Injections inject code in weakly implemented database managers and extract restricted data.

Example: ZZb00t

In April 2017, a 24-year-old German national with the pseudonym ZZb00t was arrested. The criminal investigation department of Bielefeld led the investigation against the suspect for felony aggravated computer sabotage and blackmailing. The hacker had launched multiple Distributed Denial of Service Attacks (DDoS) on institutions like DPD and DHL, demanding a ransom fee. The hacker himself was charged and found guilty of all charges and was sentenced to one year and ten months with three years of probation. Additionally, he was mandated to 100 hours of community service to serve as an example to other hackers.
ZZb00t shows signs of remorse as he pleaded to change from a grey-hat-hacker to a white-hat-hacker.

After giving an overview of the tools and attacks correlated with Network Forensics, it is time to introduce the usual further reading section.

6.7 Further Reading

Following literature is interesting for students who are looking forward to further deepen their knowledge of Network Forensics:

- **Network Forensics: Tracking Hackers through Cyberspace** - This book takes the readers on a practical ride through Network Forensics, considering both practical and theoretical topics and appropriate tooling for different tasks.
- **A Graph Based Approach Toward Network Forensics Analysis** - A paper from the University of Iowa presenting a novel graph-based approach toward network forensic analysis. This paper focuses on the evidence-based graphs and the hierarchical representation of the respective evidence.
- **Network Forensics Based on Fuzzy Logic and Expert System** - This paper presents an effective and automated analysing system for network forensics. The development of a fuzzy logic based expert system is conducted for an efficient network forensic analysis.

After the presentation of different papers and books that are worth reading on the topic of Network Forensics, a summary of the chapter is given.

6.8 Summary

This chapter has shown the Network Forensics is an especially difficult branch of Digital Forensics which is accompanied by different challenges. Special methodologies for investigations and data collection strategies were introduced and explained. A thorough explanation of relevant networking topics like detection and prevention techniques, and the ISO/OSI layer were also concluded in this chapter. Finally, a brief overview of different toolsets was given, to prepare the student for the practical exercises. As with all chapter, further reading material is provided for those students who want to know more about the topic.

Next chapter will be about Anti-Forensics, which will deal with techniques and methods that criminals use to harden the task of forensic investigators.

6.9 Review Questions

1. Define Network Forensics in your own words. State your opinion on the difficulty of Network Forensics in comparison to the other types of forensics.
2. OSCAR is not only a Hollywood trophy. Please explain what it stands for in the context of Network Forensics. Cross reference it with the pendant from Computer and Mobile Forensics.
3. What is especially difficult about Network Forensics? There is one point highlighted within the lecture, please consider that.
4. Define the following and give practical examples and implementations:
   - IPS
   - IDS
   - Honeypots
5. List the ISO/OSI layers as defined in the literature. Now forget the ISO/ISO layers, which aspects of a network connection play an important role during a forensic examination.
6. Two methods for Network Forensics were introduced. Explain them and expand the pros and contras listed within the script and slides respectively.
7. List three different properties of Network Forensic tools. Now create a high-level architecture of a tool which combines all three traits.

8. Network Forensics: Tracking Hackers through Cyberspace is an excellent book on Network Forensics. Please read at least one chapter and provide an executive summary.

9. Research the literature on Network Forensics. Provide at least one topic that can be added to the lecture which fits the topic.

10. Wireshark is the bread and butter of Network Forensics. Explain what Wireshark is used for, hint out capabilities and boundaries.

7 Anti-Forensics

In this chapter we deal with the topic of anti-forensics. In the previous chapters we learned a lot about digital forensics and its examination of evidence devices. **Anti-forensics** addresses techniques which have the major goal to make the analysis and examination of digital forensic evidence from difficult and time-consuming up to impossible. An accurate definition of anti-forensics does not exist, so it is possible that in different sources there are different descriptions. [3][56]

Anti-Forensics

"manipulate, erase, or obfuscate digital data or to make its examination difficult, time consuming, or virtually impossible" [56, p.83][3]

The classification of anti-forensic techniques is in every source different because new technologies were added or the classification is more or less detailed. But anti-forensic techniques could be divided roughly into manipulation, hiding or destruction of data. These techniques are used from all sort of criminals in order to frustrate the examiner of the evidence or to exhaust the limited money and time contingent. If the examiner finds nothing, the possibility of frustration is high. Then the examiner is pleased when at least a little, maybe planted, hint is found. The other strategy is that the examination is very time-consuming in order to exhaust the money contingent of a forensic examination.

The anti-forensic techniques are not only used by criminals. Theses techniques are also used by companies and normal persons in order to **protect their privacy and secrets**. An investigator has to know this, because a trace that an anti-forensic technique was used, is not necessarily a hint for a criminal action. Usual behaviour with anti-forensic techniques are, for example, clearing the browser history, using the private browsing mode or wiping a hard drive before selling it. The wiping of a device by a company with the aid of remote access is also a common implemented feature in order to prevent the leakage of company secrets. The encryption of a device is nowadays also a common action by companies or even by non experts in order to protect personal information from unauthorised access. So traces of the usage of anti-forensic techniques could be just a hint to look closer. [2][28][56]

In the following some selected anti-forensic techniques are introduced.

7.1 Hiding data

Hiding data is one anti-forensic strategy and works in different ways. Data could be hidden from the observer in the system by *encryption, masquerade or steganography.* These techniques make data unreadable, hide data behind data or hide even the existence of data. Concealing data is an efficient way to obfuscate data from all too curious viewers. [2][56]

7.1.1 Cryptography

Cryptography is already a few thousand years old and it has always been used to hide and protect information. This could also be a technique of a suspect in order to prevent that data finds its way into the wrong hands during an investigation. **Encryption** of single files or an entire device is not complicated anymore, even for normal users. Functions for encryption are provided by nearly every vendor of a device or an operating system. Nowadays, encryption is only one click away on a device. In the following list some encryption software is presented.

- **BitLocker** - *BitLocker* is a function for a hard drive encryption by *Microsoft.* This function is not available in all versions of Windows and it can encrypt entire hard drives as well as removable storage devices with *BitLocker To Go.* BitLocker can use a *Trusted Platform Module (TPM)* for the encryption with or without an additional password or only a password. [56]

- **FileVault** - *FileVault* is an encryption feature of the operating system Mac OS X by *Apple* since the version 10.3. *FileVault 2*, used since Mac OS X 10.7, uses an AES 128-bit encryption with a 256-bit key. The users have the opportunity to store their passphrases with Apple servers. FileVault provides, since FileVault 2, a full disk and an on-the-fly encryption. This encryption feature of Apple meets the FIPS standard. [56][57]

- **VeraCrypt** - Contrary to the other already mentioned hard drive encryption functions *VeraCrypt* is open-source software. VeraCrypt originates from the former encryption software *TrueCrypt.* The development of TrueCrypt was stopped in 2014 and in 2012 VeraCrypt was already separated based on TrueCrypt 7.1a. VeraCrypt supports an automatic on-the-fly encryption of an entire hard drive or a storage device. [74]

This can make an examination of a digital device very complicated. A **running encrypted computer system** with these mentioned encryption capabilities is often the only chance to get any data from that device as already mentioned in Chapter *Digital Forensics.*

But sometimes the encryption function forgets to encrypt some parts of a system or the system stores data at the non encrypted area and then these parts can be recovered by an examiner. So the reliability of an encryption software depends on the quality of the software.

Another possibility for a forensic examiner is to get hold of the proper **password**. To achieve this, there are also different options. The forensic scientist, for example, can address the weakest point in this construction and that is the human being himself. The first possible and easiest option is to ask politely for the password, maybe the examiner gets it from the owner of the device. But this option is not available if the owner is not known or not cooperative, then a forensic examiner is demanded. [56]

Breaking Passwords

Breaking the password is an option then. Breaking a password can be very time-consuming and difficult depending on how hard a chosen password is. Here the laziness of people often play into the hands of examiners. Completely random strings cannot be remembered by people, so we tend to choose passwords that are not of a random nature. We use, for example, birth dates, pet names and maybe our hobbies for creating passwords. For breaking a password different methods are used. One possible characteristic of an encrypted device is the option for deleting data after failed logins. A forensic investigator tries to break the encryption but before a device is completely locked or deleted the actions for breaking the pin or password are stopped. [56]

Brute Force Attack

If a forensic examiner has no clue about the owner of the device or the password, the most time-consuming option is to make a brute force attack on the password. With this attack every possible password is checked out. A brute force attack needs a lot of computing power in order to manage such an attack in a suitable time. [56]

Dictionary Attack

An easier way to break a password than by a brute force attack is a dictionary attack. A **dictionary attack** can be done by using an already existing dictionary or by creating a new one. There are different dictionaries with an accumulation of, for example, frequently used passwords or possibly used words. Otherwise a **specialised dictionary** is created with information about the owner of the device. This method covers the use of pet names and birth dates in passwords. Additionally, special words of possible criminal terms are included, for example, in child pornography cases. [56]

7.1.2 Masquerading data

Another method of obfuscating is **masquerading** by changing file extensions, names and storage locations. This technique is more complicated for users than just clicking a button for encryption. Here the user needs to know which technical details to change in order to hide the data in an efficient way. It requires more knowledge about digital data. [25][33]

In the following list a few possibilities for masquerading single files are listed.

- **File Extension** - In a Windows system the file extension is needed in order to open the file and load the right application. Otherwise the Windows system cannot open the file. A Unix based system does not depend on the file extension to open a file. A Unix system looks at the file signature at the beginning of a file which determines the file format. Unix based systems sometimes show the file extension of a file but do not need it. By changing the file extension, hiding the file behind another file type is possible. But this is easy to detect, in Unix systems it would not make any difference and in Windows systems the file cannot be opened so it would attract attention. [33]

- **File Signature** - At the beginning or at the end (or both) of a file there are blocks of characters ("magic bytes"), called *header* and *footer*, which defines the type of the file. These blocks of characters are called *file signature*. At the beginning a JPEG file, for example, has the hexadecimal code *FF D8 FF E0*. For hiding data, a change of the file signature and file extension is also usable. Here, an important image can be hidden between normal text documents which are maybe not that interesting for an examiner. For example, in a child pornography case this technique is likely because in such a case a forensic examiner often only looks for videos and images. [33]

- **File Name** - Changing *file names* is also an easy way in order to make it more difficult for an examiner. In the mass of data files in a system, an unsuspicious name helps in order to stay undetected especially in the combination with a file signature and extension change. Often downloaded files, for example, in a child pornography case are named with abbreviations commonly used in the criminal area. [28]

- **Storage Location** - Hiding data also works in the way we often do not find things again, because they are at a place were they should normally not be in the system. In a computer system there are thousands of folders and subfolders and so there is enough space to hide an important file somewhere in a completely unusual place. Combined with file signature changes the file will seem to be completely uninteresting. [33]

Data could also be hidden in places on the hard drive where a normal system does not look. These are unallocated and unreachable places for the normal system. The partition gap between two partitions is such an example. There are other areas where secret data can be stored like the *slack space* (also called file slack) or the *Host Protected Area (HPA)* of a hard drive by specialised software. [25]

If a defendant uses all these masquerading techniques together the possibility is high that a forensic investigator will overlook the file. Because often if an investigator has already found something, maybe a planted hint, the examiner will not dig deeper in the amount of data. This approach is only applicable to single files. An application to a big amount of data is too much effort.

7.1.3 Steganography

Steganography is not a new technique. It was already used in the 15th century. The Greek words *Stegos (= covered)* and *Graphie (= writing)* describes steganography in a good way. **Steganography** is a kind of writing where the existence of a secret message is hidden, but not the official communication itself.

Steganography

"The art of covered or hidden writing" [42]

Classical steganography techniques are microfilms and microdots as well as invisible ink.

There are many types of steganography like linguistic or graphical steganography. The two big parts of steganography are technical and linguistic steganography. The visual steganography is a sub part of the linguistic one. [42]

In this section we concentrate on the technical therefore the **computer-assisted steganography**.

In steganography a transport medium for the hidden message is used, so called **carrier**. The hidden message is placed in the carrier file. Common carrier file types are image files, video files and audio files, for example. But there are more file types which can be used for steganography. The carrier files are used because these types have the property of holding an amount of redundant data. It means that this data is not necessarily needed to display or to play back the file correctly. This redundant data is then replaced by the secret message. The **payload** of a carrier file, the secret message, can be everything. It does not have to be a text file. Variable combinations of file types for the carrier file and payload are possible. [25][42][56]

Applied steganography is very **difficult to detect** in a forensic investigation. A hint for used steganography could be the proper size of a file, for example. Once

steganography is detected, it is very hard to reveal the secret message. The exposure of the payload depends on the used steganography tool and the possibly used password. For extracting the payload, the examiner has to find the originally used tool because every tool has its special way to place the secret message within the carrier.

Once, the enterprise *Backbone Security* listed over 960 steganography applications [56]. Therefore, it is really difficult but necessary to find the original tool.

The detection of **steganography tools**, if they are not deleted, can also be done by matching the hash of the tool with known hash databases, a hash alignment as described already in an earlier chapter. Additionally, some carrier files could be detected by some specialised steganalysis (detection of steganography), software like *Stego Watch* and *StegDetect* for JPEG image files. Steganography software, for example, are *StegHide*, *Camouflage* and *OpenStego* [58]. StegHide, for example, uses graph theory in order to decide in which pixels the secret message should be saved [35]. [42]

In combination with cryptography steganography is a really effective way to hide data.

Example

According to *USA Today* in 2001, U.S. officials and experts announced that steganography was the newest communication method for terrorists. Osama bin Laden and his companions (al-Quaida) were accused to hide plans and maps in pornographic files on websites and in sport chat rooms. Publishing a picture with embedded secret data on the Internet is an easier way to spread a clandestine message than sending an email because here the communication itself is hidden. [41]

7.2 Destruction of Data

In order to prevent that data find its way into the wrong hands, destroying data is also an option. This option however is a definitive one.

7.2.1 Wiping Data

The deletion of data is more complicated than a usual computer user thinks. If the **delete button** is pressed, the deleted file is still there, only the link to this file was deleted. The file remains on the hard drive until it is overwritten by another file. These files can be carved out and recovered by a forensic examiner. [2][56]

But there are special software tools for wiping a hard drive which cover this problem. These **hard drive wiping tools** can operate in different modes.

The first is to wipe an entire hard drive. Here, everything on the storage device is overwritten. Another possibility is to wipe only specific files. This method has a weak

point in combination with journaling file systems. Here, the file itself is deleted on the hard drive, but maybe a copy of it remains in the journal and is then recoverable.

The wiping takes place with the use of a **sequence of characters** which can be patterns or random data. The storage area which has to be wiped is overwritten with this sequence of characters. The used sequence of characters depends on the used tool. Patterns of zeros, FFs, and random data are in use, for example. [25]

The quality of the software determines the **reliability** of the wiping tool. The wiping of an entire hard drive is often good but the wiping of just specific files is more difficult and some blocks may be forgotten. Additionally, wiping tools sometimes forget some places to overwrite, for example, the partition gap. These leftovers can be recovered by an examiner.

Different **standards** for wiping a hard drive were developed. The American *Department of Defence (DoD)*, the *National Institute of Standards and Technology (NIST)* as well as the German *Federal Office for Information Security (BSI)* determined such standards. In the standards the number of passes, used patterns and the verification of the actions are defined. The quality of erasure tools depends on the good implementation of these standards in the tools. As in cryptography, the tool is only as good as the correct implementation of the standard. [39]

The examiner can get a hint for the use of a wiping tool by the used wiping pattern or the not deleted wiping tool. Even if the tool is deleted, artefacts remain in the registry. These traces can be a hint that the owner of the device wants to hide something. [25][56]

All these different techniques could be used in order to make a forensic examination very hard or even impossible. There are still more techniques which can be used like exploiting the forensic tool itself, data falsification and data pooling. However the presented anti-forensic techniques are the most common ones. [33]

Certainly the best method for minimising our digital footprint is still the **prevention of data creation** in the first place. Data which was never there cannot be recovered by an examiner.

According to this principle the private browsing mode of web browsers is helpful because this mode produces less data than the usual mode. If this is not enough, the user can use the often suspicious viewed *Tor* browser. With this browser the user has access to *The Onion Router* network. The Tor network hides the location of the user, the visited sites and obfuscates the communication. [72]

The usage of the Tor browser does not make everything invisible what you are doing, even in the Tor network the communication can be monitored when enough nodes are viewed. And for a forensic examiner the existence of a Tor browser on a computer is always a little bit suspicious. When the judge asks an examiner if the suspect could have had the possibility to buy a weapon in the Internet and a Tor browser is found, the examiner will answer that it could be possible. So this is not a good argument for or against the proof of innocence. [49]

7.3 Further Reading

A fundamental overview over the chapter topic is given in the book [56] and in [3] as well. Further anti-forensic techniques are listed and described in the paper [33] and in the article [25]. In order to deepen the topic of a new kind of steganography the paper "Steganalysis of transcoding Steganography" [38] and for steganalysis the articles "Cyber warfare: Steganography vs. Steganalysis" [75] or "A Review of Image Steganalysis Techniques for Digital Forensics" [40] could be read.

For more information on how to hide data elsewhere, see "Data Hiding in Journaling File Systems" [20].

7.4 Summary

In this chapter you learned about anti-forensics which is defined as techniques meant to interfere with a forensic examination. But these techniques could also be used for actions with good intentions. Innocent users can use these techniques in order to prevent criminals to get all their private data by stealing or hacking their devices or by companies in order to control the unwanted leakage of company secrets.

Anti-forensic techniques can be divided roughly into manipulation, hiding or destruction of data. There are still other types of anti-forensic techniques than the presented ones.

In the section of hiding data, cryptography, masquerading and steganography is named. With the encryption of data it can be prevented that data gets into the wrong hands. Examiners have to be capable of breaking passwords and have knowledge of characteristics of passwords. Nowadays, operating systems have an encryption function available otherwise there is open-source software. Masquerading of important data is a good and easy way for concealing files in the system. Here, the manipulation of file extensions, signatures and names as well as the storage location are mentioned. These techniques in combination are effective against discovery of secret data and hard to break. Steganography is another method of hiding data. It is like cryptography an old approach for concealing data. In this method secret data is hidden in other unsuspicious data. For a forensic examiner it is hard to break this type of hiding because in order to detect the exact used tool has to be determined as well as the used password.

The other section is about the destruction of data. This approach is a definitive one to get rid of data. Here, different tools are available for wiping a complete hard drive or only eliminate single files. But this method is not perfect because some places on the hard drive are forgotten and an examiner can recover these fragments.

In general there are a lot more methods for anti-forensics and with new technology new techniques are added. So a digital forensic examiner has to be always up to date.

7.5 Review Questions

1. What is anti-forensics? Define it in your own words.
2. Which anti-forensic techniques exist?
3. How can you hide data?
4. Which is the easiest way to obtain encrypted data?
5. What do you need to keep in mind when breaking a password?
6. Which masquerading methods exist?
7. What is meant by the term “file signature”?
8. What is steganography?
9. Which problem can occur with the method of destruction of data?
10. How can an examiner determine if a wiping tool was used?

Bibliography

[1] heise online (Andreas Wilkens). *EuGH: The Pirate Bay verstößt gegen das Urheberrecht*. https://www.heise.de/newsticker/meldung/EuGH-The-Pirate-Bay-verstoesst-gegen-das-Urheberrecht-3743108.html. [Accessed 21.11.2018].

[2] A. Årnes, A. O. Flaglien, I. M. Sunde, A. Dilijonaite, J. Hamm, J.-P. Sandvik, P. C. Bjelland, K. Franke, and S. Axelsson. *Digital Forensics*. 1st ed. Wiley, 2018.

[3] J. J. Barbara. *Anti-Digital Forensics, The Next Challenge: Part 1*. Forensic Magazine. https://www.forensicmag.com/article/2008/12/anti-digital-forensics-next-challenge-part-1 [Accessed 12.02.2019]. Dec. 2008.

[4] V. Baryamureeba and F. Tushabe. *The Enhanced Digital Investigation Process Model*. Digital Forensic Research Conference. https://dfrws.org/sites/default/files/session-files/paper-the_enhanced_digital_investigation_process_model.pdf.

[5] Bayerische Polizei. *Straftaten im Internet*. Website. https://www.polizei.bayern.de/schuetzenvorbeugen/kriminalitaet/computerkriminalitaet/index.html/308 [Accessed 14.02.2019].

[6] A. Bhattacharya. *Canada is trying to solve a murder by pinging everyone whose cellphone was nearby*. 2016. URL: https://qz.com/824701/canada-is-trying-to-solve-a-murder-by-pinging-everyone-whose-cellphone-was-nearby/ (visited on 12/03/2018).

[7] Binary Intel. *Chip-Off Forensics*. URL: http://www.binaryintel.com/services/jtag-chip-off-forensics/chip-off_forensics/ (visited on 12/03/2018).

[8] Binary Intel. *JTAG Forensics*. URL: http://www.binaryintel.com/services/jtag-chip-off-forensics/jtag-forensics/ (visited on 12/03/2018).

[9] Biography.com Editors. *Philip Markoff Biography*. 2014. URL: https://www.biography.com/people/philip-markoff-438836 (visited on 12/03/2018).

[10] Bundesamt für Sicherheit in der Informationstechnik. *Leitfaden "IT-Forensik"*. Vol. Version 1.0.1. Bundesamt für Sicherheit in der Informationstechnik, Mar. 2011.

[11] Bundeskriminalamt. *Cybercrime Bundeslagebild 2017*. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2017.html [Accessed 14.02.2019]. July 2018.

[12] Bundesverfassungsgericht. *Verfassungsbeschwerden gegen § 202c Abs. 1 Nr. 2 StGB unzulässig*. https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2009/bvg09-067.html. [Accessed 15.11.2018].

[13] Cambridge Dictionary. *Definition "cybercrime"*. Entry in Cambridge Dictionary. https://dictionary.cambridge.org/de/worterbuch/englisch/cybercrime [Accessed 14.02.2019].

[14] Council of Europe. *Convention on Cybercrime*. https://www.coe.int/de/web/conventions/full-list/-/conventions/rms/0900001680081561. [Accessed 05.09.2018]. 2001.

[15] Council of Europe. *Additional Protocol to the Convention on Cybercrime*. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189. [Accessed 30.10.2018]. 2003.

[16] Council of Europe. *Chart of signatures and ratifications of Treaty 185*. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=6NIdbhd0. [Accessed 23.10.2018].

[17] Council of Europe. *Chart of signatures and ratifications of Treaty 189*. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189/signatures?p_auth=6NIdbhd0. [Accessed 23.10.2018].

[18] S. Davidoff. *Network Forensics: Tracking Hackers through Cyberspace*. Upper Saddle River, NJ: Prentice Hall, 2012. ISBN: 0-13-256471-8.

[19] Duden. *Definition "Cybercrime"*. Entry in German Duden. https://www.duden.de/rechtschreibung/Cybercrime [Accessed 14.02.2019].

[20] K. Eckstein and M. Jahnke. "Data Hiding in Journaling File Systems." In: *DFRWS*. https://www.dfrws.org/sites/default/files/session-files/paper-data_hiding_in_journaling_file_systems.pdf [Accessed 25.02.2019]. 2005.

[21] European Union. *General Data Protection Regulation*. https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&qid=1540889287896&from=DE. [Accessed 30.10.2018]. 2016.

[22] R. Fahey. *Computer Forensics: Forensic Analysis and Examination Planning*. 2017. URL: https://resources.infosecinstitute.com/category/computerforensics/introduction/areas-of-study/forensic-science/forensic-analysis-and-examination-planning/ (visited on 11/14/2018).

[23] R. Fahey. *Computer Forensics: Network Forensics Analysis and Examination Steps*. https://resources.infosecinstitute.com/category/computerforensics/introduction/areas-of-study/digital-forensics/network-forensics-analysis-and-examination-steps/ [Accessed 28.02.2019].

[24] A. O. Flaglien, A. Mallasvik, M. Mustorp, and A. Årnes. "Storage and exchange formats for digital evidence". In: *Digital Investigation* 8.2 (2011), pp. 122–128. ISSN: 1742-2876. DOI: https://doi.org/10.1016/j.diin.2011.09.002. URL: http://www.sciencedirect.com/science/article/pii/S1742287611000685.

[25] S. Garfinkel. "Anti-forensics: Techniques, detection and countermeasures". In: *2nd International Conference on i-Warfare and Security*. Vol. 20087. 2007, pp. 77–84.

[26] Gerichtshof der Europäischen Union. *Pressemitteilung Nr.64/17, Urteil in der Rechtssache C-610/15 Stichting Brein / Ziggo BV, XS4All Internet BV*. https://curia.europa.eu/jcms/upload/docs/application/pdf/2017-06/cp170064de.pdf. [Accessed 21.11.2018].

[27] P. Gershteyn, M. Davis, and S. Shenoi. "Forensic Analysis of BIOS Chips". In: *Advances in Digital Forensics II*. Ed. by M. S. Olivier and S. Shenoi. Boston, MA: Springer US, 2006, pp. 301–314. ISBN: 978-0-387-36891-7.

[28] A. Geschonneck. *Computer-Forensik (iX Edition): Computerstraftaten erkennen, ermitteln, aufklären*. dpunkt.verlag, 2014. ISBN: 9783864914904.

[29] Gesetz über Urheberrecht und verwandte Schutzrechte (UrhG). https://www.gesetze-im-internet.de/urhg/. [Accessed 30.10.2018].

[30] H. Gierow. *Computerkriminalität nimmt statistisch gesehen zu*. Article on golem.de. https://www.golem.de/news/cybercrime-computerkriminalitaet-nimmt-statistisch-gesehen-zu-1704-127477.html [Accessed 14.02.2019]. Apr. 2017.

[31] Grundgesetz. *Art. 103 Abs. 2 GG*. https://www.gesetze-im-internet.de/gg/art_103.html. [Accessed 30.10.2018].

[32] Guidance Software EnCase. *EnCase Forensic User's Guide, Version 8.07*. Website, PDF. URL: http://encase-docs.opentext.com/documentation/encase/forensic/8.07/Content/Resources/External%20Files/EnCase%20Forensic%20v8.07%20User%20Guide.pdf%20[Accessed%2026.02.2019].

[33] M. Gül and E. Kugu. "A survey on anti-forensics techniques". In: *2017 International Artificial Intelligence and Data Processing Symposium (IDAP)*. Sept. 2017, pp. 1–6. DOI: 10.1109/IDAP.2017.8090341.

[34] D. Heinson. "IT-Forensik - Zur Erhebung und Verwertung von Beweisen aus informationstechnischen Systemen". https://kobra.bibliothek.uni-kassel.de/handle/urn:nbn:de:hebis:34-2016110751250 [Accessed 30.10.2018]. Dissertation. Verlag Mohr Siebeck, Tübingen: University Kassel, 2015.

[35] S. Hetzl. *Steghide - manual*. http://steghide.sourceforge.net/documentation/manpage.php [Accessed 21.02.2019]. May 2002.

[36] F. Imam. *Common Mobile Forensics Tools and Techniques*. 2017. URL: https://resources.infosecinstitute.com/category/computerforensics/introduction/mobile-forensics/common-mobile-forensics-tools-and-techniques/ (visited on 12/03/2018).

[37] Interpol. *Cybercrime*. Website. https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime [Accessed 14.02.2019].

[38] A. Janicki, W. Mazurczyk, and K. Szczypiorski. "Steganalysis of transcoding steganography". In: *annals of telecommunications - annales des télécommunications* 69.7 (Aug. 2014), pp. 449–460. ISSN: 1958-9395. DOI: 10.1007/s12243-013-0385-4. URL: https://doi.org/10.1007/s12243-013-0385-4.

[39] K. M. Jefcoat. *A comprehensive List of Data Wiping and Erasure Standards*. https://www.blancco.com/blog-comprehensive-list-data-wiping-erasure-standards/ [Accessed 12.02.2019]. Oct. 2017.

[40] K. Karampidis, E. Kavallieratou, and G. Papadourakis. "A review of image steganalysis techniques for digital forensics". In: *Journal of Information Security and Applications* 40 (2018), pp. 217–235. ISSN: 2214-2126. DOI: https://doi.org/10.1016/j.jisa.2018.04.005. URL: http://www.sciencedirect.com/science/article/pii/S2214212617300777.

[41] J. Kelley. *Terror groups hide behind Web encryption*. Website USA Today. https://usatoday30.usatoday.com/life/cyber/tech/2001-02-05-binladen.htm [Accessed 12.02.2019]. Feb. 2001.

[42] G. C. Kessler. *An Overview of Steganography for the Computer Forensics Examiner*. https://commons.erau.edu/cgi/viewcontent.cgi?article=1138&context=publication [Accessed 05.02.2019]. Feb. 2015.

[43] D. Kostadinov. *The Mobile Forensics Process: Steps & Types*. 2017. URL: https://resources.infosecinstitute.com/category/computerforensics/introduction/mobile-forensics/the-mobile-forensics-process-steps-types/ (visited on 12/03/2018).

[44] M. Lutz. *Tatwaffe Computer – Schaden geht in die Milliarden*. Article on WELT. https://www.welt.de/politik/deutschland/article175740321/Computerkriminalitaet-steigt-Milliardenschaeden-fuer-Firmen.html [Accessed 14.02.2019]. Apr. 2018.

[45] heise online (Martin Holland). *DSGVO-Verstoß: Krankenhaus in Portugal soll 400.000 Euro zahlen.* https://www.heise.de/newsticker/meldung/DSGVO-Verstoss-Krankenhaus-in-Portugal-soll-400-000-Euro-zahlen-4198972.html. [Accessed 26.11.2018].

[46] R. Minutaglio. *The BTK Killer Brutally Murdered 10 People. In Chilling New Audio, He Explains Why.* 2018. URL: https://www.esquire.com/entertainment/a22812299/where-is-btk-killer-dennis-rader-today/ (visited on 12/03/2018).

[47] OccupyTheWeb. *Digital Forensics for the Aspiring Hacker, Part 5 (Windows Registry Forensics).* 2015. URL: https://null-byte.wonderhowto.com/how-to/hack-like-pro-digital-forensics-for-aspiring-hacker-part-5-windows-registry-forensics-0160561/ (visited on 11/14/2018).

[48] heise online. *The Pirate Bay.* https://www.heise.de/thema/The-Pirate-Bay. [Accessed 21.11.2018].

[49] heise online. *Tor Browser 8.0.5.* https://www.heise.de/download/product/tor-browser-40042 [Accessed 07.02.2019].

[50] M. Pollitt. "Applying Traditional Forensic Taxonomy to Digital Forensics". In: *Advances in Digital Forensics IV*. Ed. by I. Ray and S. Shenoi. Boston, MA: Springer US, 2008, pp. 17–26. ISBN: 978-0-387-84927-0.

[51] S. Prather. *Minnesota detectives crack the case with digital forensics.* 2014. URL: http://www.startribune.com/when-teens-went-missing-digital-forensics-cracked-case/278132541/ (visited on 12/03/2018).

[52] Pressemitteilung des Bundeskriminalamtes. *Zahlen und Fakten zur Bekämpfung der Kinderpornografie.* https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2018/Presse2018/180606_KinderpornografieKlarstellung.html;jsessionid=.live0601?nn=29858. [Accessed 21.11.2018].

[53] Rechtsanwalt und Strafverteidiger Dr. Böttner. *Überblick über die Gesetzesänderungen 2015.* https://www.rechtsanwalt-sexualstrafrecht.de/ueberblick-ueber-die-gesetzesaenderungen-2015/. [Accessed 13.11.2018].

[54] M. Reith, C. Carr, and G. Gunsch. "An examination of digital forensic models". In: *International Journal of Digital Evidence* 1.3 (2002), pp. 1–12.

[55] M. Rouse. *network forensics.* https://searchsecurity.techtarget.com/definition/network-forensics [Accessed 28.02.2019].

[56] J. Sammons. *The Basics of Digital Forensics: The Primer for getting started in Digital Forensics.* 2nd ed. Syngress, 2015.

[57] K. Scarfone. *Apple FileVault 2: Full disk encryption software overview.* https://searchsecurity.techtarget.com/feature/Apple-FileVault-2-Full-disk-encryption-software-overview [Accessed 31.01.2019]. 2015.

[58] P. Shankdhar. *Best Tools to perform Steganography*. [Accessed 05.02.2019]. Feb. 2018. URL: https://resources.infosecinstitute.com/steganography-and-tools-to-perform-steganography/#gref.

[59] spomedial - Sportmedizin interaktiv lernen. *Tannerstadien*. http://vmrz0100.vm.ruhr-uni-bochum.de/spomedial/content/e866/e2442/e9012/e9017/e9153/e9171/index_ger.html. [Accessed 14.11.2018].

[60] Strafgesetzbuch. *§1 Keine Strafe ohne Gesetz StGB*. https://www.gesetze-im-internet.de/stgb/__1.html. [Accessed 23.10.2018].

[61] Strafgesetzbuch. *§184b Verbreitung, Erwerb und Besitz kinderpornographischer Schriften StGB*. https://www.gesetze-im-internet.de/stgb/__184b.html. [Accessed 30.10.2018].

[62] Strafgesetzbuch. *§202a Ausspähen von Daten StGB*. https://www.gesetze-im-internet.de/stgb/__202a.html. [Accessed 20.11.2018].

[63] Strafgesetzbuch. *§202b Abfangen von Daten StGB*. https://www.gesetze-im-internet.de/stgb/__202b.html. [Accessed 20.11.2018].

[64] Strafgesetzbuch. *§202c Vorbereiten des Ausspähens und Abfangens von Daten StGB*. https://www.gesetze-im-internet.de/stgb/__202c.html. [Accessed 30.10.2018].

[65] Strafgesetzbuch. *§263a Computerbetrug StGB*. https://www.gesetze-im-internet.de/stgb/__263a.html. [Accessed 20.11.2018].

[66] Strafgesetzbuch. *§269 Fälschung beweiserheblicher Daten StGB*. https://www.gesetze-im-internet.de/stgb/__269.html. [Accessed 20.11.2018].

[67] Strafgesetzbuch. *§303a Datenveränderung StGB*. https://www.gesetze-im-internet.de/stgb/__303a.html. [Accessed 20.11.2018].

[68] Strafgesetzbuch. *§303b Computersabotage StGB*. https://www.gesetze-im-internet.de/stgb/__303b.html. [Accessed 20.11.2018].

[69] Strafgesetzbuch. *(StGB)*. https://www.gesetze-im-internet.de/stgb/. [Accessed 05.09.2018].

[70] Strafprozessordnung. *§72 ff. StPO*. https://www.gesetze-im-internet.de/stpo/__72.html. [Accessed 30.10.2018].

[71] T3k Forensics. *10 Challenges in Mobile Forensics*. URL: http://www.t3k-forensics.com/allgemein-en/10-main-challenges-in-mobile-forensics2/ (visited on 12/03/2018).

[72] Tor Project. *Tor Browser*. https://www.torproject.org/projects/torbrowser.html.en [Accessed 07.02.2019].

[73] United Nations. *Convention on the Rights of the Child*. https://www.ohchr.org/en/professionalinterest/pages/crc.aspx. [Accessed 20.11.2018].

[74] VeraCrypt. *VeraCrypt Homepage*. https://www.veracrypt.fr/en/Home.html [Accessed 05.02.2019].

[75] H. Wang and S. Wang. "Cyber warfare: steganography vs. steganalysis". In: *Communications of the ACM* 47.10 (2004), pp. 76–82.

[76] Warlock. *File Carving*. 2014. URL: https://resources.infosecinstitute.com/file-carving/ (visited on 11/18/2018).

[77] Welt. *"Müssen davon ausgehen, dass sich Missbrauch Tausender Kinder unerkannt fortsetzt"*. https://www.welt.de/vermischtes/article176176459/Kinderpornografie-Muessen-davon-ausgehen-dass-sich-Missbrauch-Tausender-Kinder-unerkannt-fortsetzt.html [Accessed 21.11.2018].

[78] Zivilprozessordnung. *§402 ff. ZPO*. https://www.gesetze-im-internet.de/zpo/__402.html. [Accessed 31.10.2018].