1. Appropriate definitions for the classical and digital Forensics, and their targets:

Digital Forensics is recovery, investigation, examination and analysis of digital material found in digital devices. Can be used in criminal cases, civil disputes, human resources/employment proceedings.

Electronic evidence can be collected from a wide array of sources, such as computers, smartphones, remote storage, unmanned aerial systems, shipborne equipment, and more.

The main target of digital forensics is to extract data from the electronic evidence, process it into actionable intelligence and present the findings for prosecution. All processes utilize sound forensic techniques to ensure the findings are admissible in court.

2. The definition of a digital crime scene and how to act there:

A place where the crime was committed, place where the device or devices where present or used as an instrument of crime.

- The scene of crime has to be frozen. Evidence has to be collected as early as possible, and without any contamination.
- Chain of custody has to be present(continuity of evidence). It has to be clear what has happened to the exhibit between it is collection and appearance in court, better should not be changed.
- All procedures used in examination should be auditable. Independent expert should be able to track all the investigations carried out by the prosecution's experts.

3. The significance of information systems (IT systems) for criminal prosecutions:

- **Big Data**

Big data is an important part of every industry, as the world generates 2.5 quintillion bytes of data a day, according to IBM. Data collection in criminal justice helps legal experts in several ways. For example, DNA and fingerprints can be stored in databases and used to identify suspects more quickly. Data can also help law enforcement recognize crime trends and take appropriate action.[4]

- **Rapid Identification Systems:**

Allow police officers to quickly see the criminal history of individuals through a basic search. People pulled over while driving without a license can still be identified instantly through an in-car computer search.[4]

- **Drones:**

When police need an aerial view of a scene, drones can help law enforcement safely observe an area.

- **Global Positioning Systems (GPS):**

GPS helps police officers get to crime scenes or locate criminals more easily. It can also be used in order to record the location history of the criminals.[4]

- **Gunshot technology:**

Gunshot technology detects gunfire and gives police officers instant access to shooting location maps, as well as information on how many shooters are present and how many shots were fired.

- **License plate scanning:**

Automatic license plate scanning technology enables police officers to instantly see if a car in their area has been stolen or if there is a warrant out for the arrest of the driver. The police department in Camden, New Jersey uses license plate readers to flag vehicles that have been a part of a drug transaction, according to the Future Trends in Policing Report by the Police Executive Research Forum and U.S. Department of Justice.

- **Surveillance cameras:**

Surveillance cameras can capture the events in a particular area and provide law enforcement with valuable insight.

- **Storage devices:**

Personal Computers, Laptops, Smartphones, USB sticks and tablets may store the needed data. Even if the criminals try to delete it. It may be restored using the file carving techniques.[4]

4. The services offered by Forensics experts, the required skills and competences of Forensics experts, and the tools applied by them to offer the services:

The basic requirement for any forensics expert is to capture and record the data and then review and examine the data to produce evidence of the issue or activity.

Key skills for forensic scientists:

- Logical and independent mind
- Meticulous attention to detail
- Excellent written and oral communication skills
- Objectivity and sensitivity when dealing with confidential information
- Ability to work under pressure and to a deadline
- Concentration and patience
- Ability to deal with stressful and emotional situations
- Confidence in your own judgement

5. The generic process (course of actions) of a Forensics examination (you may refer to SAP, CFIP, IDIP, BSI, etc.) and a checklist for Forensics experts:

The computer forensics specialist will take several careful steps to identify and attempt to retrieve possible evidence that may exist on a subject computer system:

- **Protect the subject computer system** during the forensic examination from any possible alteration, damage, data corruption, or virus introduction.
- **Discover all files on the subject system.** This includes existing normal files, deleted yet remaining files, hidden files, password-protected files, and encrypted files.
- **Recover** of discovered deleted files.
- **Reveal** the contents of hidden files as well as temporary or swap files used by both the application programs and the operating system.
- **Accesses the contents** of protected or encrypted files.
- **Analyze all possibly relevant data** found in special areas of a disk. This includes unallocated space on a disk (currently unused, but possibly the repository of previous data that is relevant evidence), as well as slack space in a file (the remnant area at the end of a file, in the last assigned disk cluster, that is unused by current file data but once again may be a possible site for previously created and relevant evidence).
- **Print out an overall analysis** of the subject computer system and listing of all possibly relevant files and discovered file data. Further**, provide an opinion** of the system layout. The **file structures** discovered. Any discovered data and **authorship information**. Any **attempts to hide, delete, protect, or encrypt information**. And **anything else** that has been discovered and appears to be **relevant** to the overall examination.
- Provide **expert consultation** and/or testimony.

6. The legal aspects of Digital Forensics: name the respective laws, i.e. Criminal Law (StGB), Corporate Law (AktG, GmbhG), Data Protection Law (GDPR), Personal Rights (KUG, BetrVG), as well as their impacts on Forensics examinations and concrete details on how to ensure legal compliance

As conventional investigators require knowledge of the law, in digital forensic there is a significant need to have Legal knowledge as well which pertains to the digital world. In an event of a cyber-attack and cybercrime, digital

Forensics experts have to take the results (digital evidence) of their findings to court for legal proceedings. This is where the digital world collides with the legal world. As digital forensics is relatively a new field and there is still work that needs to be done regarding cyber laws, forensics experts have to continuously adapt newly created or changing laws related to cybercrime. Forensics investigators must also adopt procedures that adhere to the standards of admissibility for evidence in a court of law.

One of the interesting parts is **corporate law**, specifically legal liability laws in relevance to the digital world. Every country has its own corporate laws which is designed to dictate the formation and the activities of corporations. Digital experts are made to abide by these corporate laws in order to not infringe the rights of a company.

The digital forensics field is affected by various laws. Every country has its own set of laws which is designed to dictate the formation and the activities. The relevant laws in Germany are: Criminal Law (StGB), Corporate Law (AktG, GmbhG), Data Protection Law (GDPR), Personal Rights (KUG, BetrVG).

- ## Criminal Law

A set of laws that aims to ensure that digital forensics experts may not commit criminal acts

in their field of work, for example: a digital forensics expert may not blackmail/ or use

phishing -/on natural persons in order to get more evidence

Section 201 Violation of spoken word:

• Recording of private communication (without permission) and making it available to someone is punishable up to 3 years imprisonment or a fine.

• Anyone as a public official that violates the privacy of spoken word will be punished up to 5 years by imprisonment or to be fined.

• The attempt to record will be punishable.

Section 201 Violation of intimate privacy by taking photographs or other images:

• Anyone who takes images of another person and/or makes it available to someone else, and/or transmits it without a permission will be punished up to 2 years by imprisonment or a fine.

• Anyone who take photographs of a person under 18 years of age in naked state (for themselves or for anyone else) will be punished up to 2 years by imprisonment or to be fined.

Section 202 Violation of the privacy of the written word:

• Any unauthorised access (not intended for the person that accessed the data) to the written documentation is punishable up to 1 year imprisonment or to be fined, especially the sealed ones.

Section 202a Data espionage:

• Any unauthorised access to the data that was especially protected against unwanted access (sealed, warning on the door, locked) and the protection (e.g., Seal, lock…) was removed is punishable up to 3 years of imprisonment or to be fined.

• Section 202a of the Criminal Code covers, among other things, software theft, data spying, economic treason and obtaining company secrets.

• Only data that is not intended for the perpetrator and is specially secured (passwords, firewall, magnetic cards, data encryption…) against unauthorised access is protected.

• Examples: key-logging Trojans, man in the middle attack N.B. File Recovery Transfer of ownership of a storage medium has nothing whatsoever about the transfer of ownership of the data inside

Section 202b Phishing

• Any phishing activities that involve obtaining data that was not intended for the individual(s) or other people by technical means will be punished up to 2 years of imprisonment or to be fined.

Section 202c Acts preparatory to data espionage and phishing

• Anyone who prepares to commit an offence under 202a & 202b by recording, selling, spreading, phishing for himself of someone else use or making accessible:

a) passwords or any other security codes that allow access to data (202a)

b) make/pass software for the committing the offence will be punished up to 1 year or to be fined.

Section 202d Handling stollen data

• Any uses or passes data to other people that was accessed unlawfully for any of usage that involves harming another person or gaining something from this act will be punished up to 3 years of imprisonment or to be fined.

Section 203 Violation of private secrets

• Anyone who is in the profession such as physician, dentist, pharmacist, lawyers, provider os legal service, psychologist, etc. discloses another person's secret such as personal, business or trade will be punished up to 1 year of imprisonment or to be fined.

• If the acts driven by self-enrichment or someone else's or intention to harm another person will be punished up to 2 years of imprisonment or to be fined.

• For a forensic expert, the relevant part of section 203 is knowing that when working with specific groups they must be particularly careful not to put the data they have access to in a risky situation.

Section 303 Criminal damage

• Damages or destruction of someone's belongings without permission from the owner (even with the permission must make sense) or

• Any alterations of the appearance of those objects as well as its attempt will be punished by up to 2 years of imprisonment or to be fined.

Section 303a Data tampering

• any unlawful alteration, deletion, rendering data (section 202a) or its attempt will be punished by up to 2 years of imprisonment or to be fined.

Section 303b Computer sabotage

• any interference with the data processing operations that has an importance to another party

1. offence related to section 303a (data tampering) or
2. transmitting or entering data under section 202a(2) with the intention to harm another or
3. damaging, destroying, rendering unusable (data could not be used as intended

anymore), removing or altering data processing system or its carrier will be

punished by up to 3 years of imprisonment or to be fined.

• in case of substantial importance to a company/organisation/public authority as well as its attempt the imprisonment could go up to 5 years or to be fined.

(e.g., Denial-of-Service (DoS) attack: attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users of the service or resource they expected.)

Section 303c Request to prosecute

• In cases under sections 303 to 303b the offence may only be prosecuted if requested, to when the prosecuting authority decides that the prosecution is needed because of the public interest.

- ## Corporate law

Set of laws which ensures that Company take required risk management measures to ensure the protection of company's assets in a case of external or internal cyber-attack. It means that trained digital forensic specialist is desirable and needed to be in disposal in order to help to prevent the crisis, to face and react to a crisis, to mitigate a damage, to assess the damage, repair and record but may not unlawfully infringe on the system of rules, practices, and processes by which a company is directed and controlled, for example: a digital forensics specialist may not interrupt practices of a company without authorisation, in order to benefit themselves.

Sector 91 AktG (Organisation, Accounting)

The Management Board must take appropriate measures, including the establishment of a monitoring system, so that any event that could threaten the company's continued existence can be identified at an early stage.

- Forensic Readiness is crucial to any organisation, as it will provides a foundation for how circumvent any altercation event and ensure business continuity.

Section 43 GmbH Directors 'liability

- The directors shall conduct the company's affairs with the due care of a prudent businessman
- Directors who breach the duties incumbent upon them shall be jointly and severally liable to the company for any damage arising
- As punishment, directors shall be obligated to compensate with fines if the damages to the company are caused by their lack of appropriate actions or inability to act correctly in event of a crisis.

To understand more why risk management is crucial, an organisation may face some of these serious threats that exist in the real world from external and internal sources but not limited:

1. Theft of proprietary information (a trade secret, information companies wish to keep confidential)
2. Sabotage of data or networks (deliberately destroy, damage, or obstruct)
3. System penetration from outside source
4. Financial fraud
5. Sexual harassment
6. Allegations of discrimination
7. Wrongful termination claims

Internals threat sources

In majority of cases the sensitive data is easily accessed by employees within the organisation and in many cases the access to corporate information is unauthorised.

As computers become more relevant in business world and employers must safeguard critical business information and make sure that his/her employees do the same. It could be one of the bad case scenarios where a discontented individual might try to damage, destroy, or misuse the important data.

The evidence could be found in electronic mail systems, on network servers, individual employee's computers. Let's not forget the fact that the computer data could be easily manipulated, trained professional(s) are needed to perform searches and appropriate analysis to identify modified data.

One of the procedures that could take place in the companies before an individual's last official working day, a forensic specialist has on-site visit where a duplicate of data on that particular individual's computer is made to ensure that the employer is protected in case where the employee choses to do anything to that data before leaving a company. The evidence can be recovered, deleted, or damaged files could be replaced in those cases where the employer is falsely accused by an employee. The trained forensic specialist could find out motives and interpret the clues what were left behind by an employee. The employee could try to delete thefiles, reformat the disc(s) or to do other things to hide or destroy the evidence. The forensic specialist might need to find out what websites have been visited, what have been downloaded,what and when files have been accessed, attempts to destroy, conceal, or fabricate evidence.

The machines such as printers and faxes could also be used in digital forensics as they could contain evidence copies that were deleted from other sources. The business emails that were backed up and preserved for months or years could also be helpful in many cases.

Electronic surveillance

Another yet important step in risk management is to prevent or record the crime using electronicsurveillance where theft, burglary, property information and trade secrets embezzlement, inappropriate employee actions are caught up in action. A director could ask his/her forensic expert to install cameras in every appropriate location such as indoors, outdoors, offices, meeting rooms, warehouses, etc.

By using video surveillance directors could protect themselves and a company interest in situations where employees are stilling time, property, secrets, or misuse company computers and take appropriate actions against the employees.

Director's computer forensics expert could also use the equipment that allows to sweep theoffice for listening devices as there are many bugging devices ranging from micro-miniature transmitters to micro miniature recorders.

The suspected fraud within the company could be uncovered at the early stage if a regular examination of computer data is in place (with the combination of surveillance and other tools) and save a lots of company finances avoiding the fate of Vogon International Limited. The abuseof power in the company where fraudsters were in the position to authorise the payments to a fictitious company and involve another member of the company. That is the reason where the directors must ensure that the regular checks are in place and those trusted with the power willnot abuse it.

Another concern arises around the correct and secure erasure where the sensitive data about the clients is licked due to incorrect deletion. The forensic expert knows better that if the data has more value than a drive it would be wise to destroy the drive.

Externals threat sources and cyber attacks

Another story when a cyber-attack happens, and IT security measures were not enough. Using traces left by the attackers, the forensic expert identifies the attack vectors and assess the extent of the damage as an incident response. This allows attacks to be reconstructed, the exploited vulnerabilities in the IT infrastructure to be identified and subsequently closed. When an incident occurs, systems across the enterprise are scanned for identified traces of compromise. The goal is to identify the patient zero. Another possible goal is root-cause analysis (RCA). Then the countermeasures could be initiated as well as the protective mechanisms are built to prevent future attacks through the same gateway.

There are many cases where hackers targeting a company's sensitive data or money. A classic gateway is an email with infected attachments or links (Phishing). It is also the Director's responsibility to make sure that there are trainings in place where the employees learn to recognize the attacks as such. Attacks are mostly targeted via so-called spear phishing or are run as large-scale campaigns across the board to exploit gaps in

systems.

Since every incident and every system is different, the methodology to be applied depends on the attack and the environment. Forensic expert would use a range of established digital forensics tools. This can be roughly divided into three parts: Endpoint Forensics analyses devices such as servers, workstations, or computers to detect traces of attacks such as malware, data exfiltration or conspicuous user behavior. Network Forensics includes the identification and analysis of attack traces based on network traffic. Malware Forensics includes the analysis of (potential) malware to identify IOC, the reconstruction of the attack process, and the assessmentof the extent of damage.

Directors are rarely wanting to hire experts from outside and trust them with company's sensitive information when the measures could be taken on regularly basis beginning with prevention of crisis by a company's forensic expert (of course if they can afford one). There is technical knowledge as well as knowledge of law and experience needed for a forensic expert toperform so many crucial tasks to protect a company. Directors of big companies might hire one or even a team to fulfil his/her legal requirement that involve digital expertise.

Section 87 BetrVG (Right of co-determination)

- The workers have a right to participate in decision-making processes of company's which concerns their work place rights. They are allowed bargain for their rights.
- A working council is set up to negotiate and ensure that any discrepancies regarding the rights of workers are noted to the organisation's management.
- When it comes to a forensics expert investigation, negotiation and terms have to take inconsiderations the elements subjected to co-determination. The employer is the subjectwho must ensure that co-determination is being respected.
- The employees have the right in the decision-making process when it comes to:

  1) Devices used to monitor employees and their data, for e.g. Camera systems, log-in/outsystems, finger-print scanners and web browser logs.

➢ Personal rights/Intellectual Property rights

A set of laws to protect the personal rights of EU citizens, in particular rights concerning their personal data in general (images, videos, audio files etc.).Moreover It aims to protect the work and the legal intellectual properties of natural and legal persons, such as scientific and artistic works This is relevant to digital forensics in the sense of prohibiting digital forensics experts fromunlawfully accessing and/or distributing personal data of natural persons as well as legal persons(companies, partnerships, etc.)

Article 2 UrhG(Protected works)

- Concerns the , publication, or altering of protected works; which encompass a variety ofitems such as works of language (which oddly includes computer programs), musical works, artistic works (such as architecture), etc.
- The protected works(intellectual property) shall only be used or modified with the owner's authorisation.
- Digital forensic specialist may not use computers tools to their benefit without authorisation or license from the owner. I.e., digital forensic experts should always get a license before using a new tool (definitely do not use pirated software), they should alsomake sure of what this license includes for e.g., are they allowed to use it forever or allowed to modify it, etc.

§ 22 kunstUrhg (Section of Art Copyright Law)

- Portraits by artists may only be put on display only with the consent of the person portrayed.
- Taking Photographs even without publishing may constitute as a violation of right to privacy.
- If the person depicted in the portrait or photograph is dead, the consent of the relatives of the person depicted is required for a period of 10 years.
- Imprisonment for up to a year or with a fine if anyone disseminates an image or publish it without consent of the person.

Privacy and data protection

The set of laws which ensures that personal data will not be professionally used without consent or a contract from the owner of that data. One very known example is collecting/using browser cookies on internet websites.

EU General Data Protection Regulation (GDPR)

- Everyone has a right to the protecting of their personal data. The processing of such personal data is obligated to be protected.
- The processing of personal data is designed to serve man; the principles and rules on the protection of individuals with regard to the processing of their personal data should, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably their right to the protection of personal data. It should contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, the strengthening and the convergence of the economies within the internal market, and the wellbeing of individuals.

Article 4 GDPR (Definitions)

- **Data subject**: The data subject is intended to be a physical person who shares his or her personal data with others, particularly organisations.
- **Personal data**: Any information related to the data subject.
- **Processing:** means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as recording, structuring, transmission, etc.

Article 6 GDPR (Lawfulness of processing)

- A set of rules to ensure that the act of processing personal data is done lawfully. This section states a variety of situation, in which processing personal data is considered legal, such as:
    a. The consent of the individual
    b. Performance of a contract
    c. Compliance with a legal obligation
    d. Necessary to protect the vital interests of a person
    e. Necessary for the performance of a task carried out in the public interest; or

f. In the legitimate interests of company/organisation (except where those interests are overridden by the interests or rights and freedoms of the data subject)

- Firstly, to process personal data it should have a legal basis and secondly, the forensics expert must make a **contract** with the Data subject which clearly states the that subject grants permission to alter, used, or publish etc the data depending on the situation.

Article 25 GDPR (Data protection by design and by default)

- This article can be used to assess the legality of processing data. An Organisation should implement appropriate techniques to ensure that data-protection principles are implemented in the act of processing said data, and to ensure that all legal requirements are met before/while/after processing that data
- It should be ensured by the organisation that only personal data which are necessary for each specific purpose of the processing are processed.
- A digital forensics expert has to consider this while processing data to know how to complete the processing lawfully. A digital forensics expert has to identify the state of the art, scope, nature, cost of implementation and the purpose of processing the data.

Article 32 GDPR (Security of processing)

- Its goal is to ensure that the process of collecting, and processing data is safe and secure.
- Processing the data should not infringe on other rights or freedoms of natural persons, that is why the collector should implement technical methods and organisational measures that ensure a level of data security appropriate for the level of risk presented by processing personal data
- Data security measures that should be taken;

1. Encrypting the data and referring to it by an alias
2. Ensuring the ongoing confidentiality, integrity, availability, and resilience of processing the systems.
3. Guaranteeing the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
4. devising a process for regularly testing, assessing, and evaluating the effectiveness of technical measures for ensuring the security of the processing

Best Practices

Specified set of practices that digital forensics experts can and should use in order to practice their work without breaking the law. For example: there is a set of procedures specified in the ISO 27002 documents (ISO 27002/16.1.1), that digital forensics experts can/should follow.

16.1.1 Responsibilities & Procedures

Organisations must ensure that the procedures should be established for a quick, effective, and orderly response to the information security incidents.

16.1.3 Reporting information security weaknesses

Prior to the engagement of services, both employees and contractors must be made aware that all security incidents need to be reported. Example: if someone is not able to access any information (availability issue)

it should be reported.

16.1.4 Assessment of and decision on information security events 20

Information security events shall be assessed thoroughly and determine if the incidents areclassified as security incidents or not.

16.1.7 Collection of evidence

The organisation will define, obtain, procure, and retain information as documentation and implement procedures. Where the organisation identified that a security incident may result inlegal or disciplinary action, they should carry out the collection of evidence carefully, ensure a good chain of custody and avoid any threat of being caught out by poor management.

Conclusion

Digital forensics is a broad and necessary field of work, and while it is becoming very much used for legal purposes, there are still a lot of laws and rules that ensure its legality at every step of every process. Therefore, it is only obvious that experts have to have good knowledge of the lawsconcerning their field of work. They should use common sense and legal advice to ensure that their work is completely legal, and they should follow the specified rules in each step of the way. They should implement technical methods that ensures keeping their processes lawful. And they should't unlawfully use illegal means to complete their work whatever the purpose might be.
They should assess, test, evaluate and document their processes, moreover they must keep the consequences in mind and take responsibility in case of an unexpected event that has been induced by their methods.

7. The meaning of contracts between companies and Forensics experts as well as a sketch of the main contents of such contracts:

Generic process for Forensics experts:

1. **Data seizure:**

Federal rules of civil procedure let a party, or their representative inspect and copy designated documents or data compilations that may contain evidence.

2. **Data duplication and preservation:**

The data must not be altered in any way, and the seizure must not put risk. Computer forensics experts should make an exact duplicate of the needed data.

3. **Data recovery:**

Computer forensics experts should be able to safely recover and analyze otherwise inaccessible evidence. Recover lost evidence is made by understanding storage technologies.

4. **Document searches**

Your computer forensics experts should also be able to search over 200,000 electronic documents in seconds rather than hours. The speed and efficiency of these searches make the discovery process less complicated and less intrusive to all parties involved.

5. **Media conversion**

Some data is stored on old and unreadable devices. Computer forensics experts should extract the relevant data from these devices, convert it into readable formats, and place it onto new storage media for analysis.

6. **Expert witness services**

Computer forensics experts should be able to explain complex technical processes in an easy-to-understand fashion. This should help judges and juries comprehend how computer evidence is found, what it consists of, and how it is relevant to a specific situation.

7. Computer Evidence Service Options

Computer forensics experts should offer various levels of service, each designed to suit your individual investigative needs. For example, they should be able to offer the following services:

- **Standard service**
- **On-site service**
- **Emergency service**
- **Priority service**
- **Weekend service**

- **Standard Service:**

Forensics expert should be able to work during normal business hours. They must ensure that equipment will still be functional after the work is done.

- **On-Site Service**

They must be able to travel to your location do computer evidence services. On-Site they has to be able to produce exact duplicate of the data storage. They have to be able to produce their services on duplicate, in order to not disrupt the business and computer. Experts should also be familiar with the Federal Guidelines for Searching and Seizing Computers and be able to help federal marshals with that.

- **Emergency Service**

Expert should be able to give highest priority in their laboratories. They has to be able to work without any interruptions.

- **Priority Service**

Forensics experts should be able to work on your case during business hours: 8:00 A.M. to 5:00 P.M., Monday through Friday. During priority services mostly the processing time can be 2 times faster.

- **Weekend Service**

Experts should be able to work from 8:00 A.M. to 5:00 P.M., Saturday and Sunday, until evidence objectives are met. Weekend Service depends on the accessibility of computer forensics experts [1]

- **Other Miscellaneous Services**

Services Computer forensics experts should also be able to provide extended services. These services include

- Analysis of computers and data in criminal investigations
- On-site seizure of computer data in criminal investigations
- Analysis of computers and data in civil litigation.
- On-site seizure of computer data in civil litigation
- Analysis of company computers to determine employee activity
- Assistance in preparing electronic discovery requests
- Reporting in a comprehensive and readily understandable manner
- Court-recognized computer expert witness testimony
- Computer forensics on both PC and Mac platforms
- Fast turnaround time

8. The basics of Forensics documentation: the most important documents and description of their contents:

All processes to collect and gather the evidence should be duly documented according to applicable procedural and legal requirements. To do this, you must keep an exhaustive record of the location and original condition of the devices.

The following are examples for proper documentation of the scene:

- Laptop computer: evidence number EVI001
- Internal hard drive: evidence number EVI001A

- USB Thumb drive: evidence number EVI001B
- DVD: evidence number EVI001C

For each device, the following data must be documented:
- Type: Computer, hard drive, flash drive, DVD, etc.,
- Brand and model
- Storage capacity, indicating if it is MB, GB or TB
- Serial number
- State: Damaged, on, off, etc.,
- Location: Stay and specific place
- Security: Access password, PIN
- Comments: Used only by children, not connected to the Internet, etc.,

They will be used in the subsequent analysis of the devices. [2]

9. A description of how a company should prepare the information systems in order to support Digital Forensics examinations: introduce and explain the term 'Forensics Readiness

Forensic Readiness -is the achievement of an appropriate level of capability by an organization in order for it to be able to collect, preserve, protect and analyze digital evidence so that this evidence can be effectively used in any legal matters, in disciplinary matters, in an employment tribunal or court of law.

Or the ability of an organization to maximize its potential to use digital evidence while minimizing the cost of an investigation

A forensic readiness plan should have the following goals:

- To gather admissible evidence legally without interfering with business processes
- To gather evidence targeting potential crimes and disputes that could have adverse impact on an organization
- To allow investigations to proceed at costs proportional to the incident
- To minimize interruption of operations by investigations
- To ensure that evidence impacts positively on the outcome of any legal action [3]

10. A detailed description of your personal Forensics Field Set and a short sketch how to install and configure it from scratch:

Forensic investigation often includes analysis of files, emails, network activity and other potential artifacts and sources of clues to the scope, impact and attribution of an incident.

- **Disk analysis: Autopsy/the Sleuth Kit**

Autopsy and the Sleuth Kit are likely the most well-known forensics toolkits in existence. The Sleuth Kit is a command-line tool that performs forensic analysis of forensic images of hard drives and smartphones. Autopsy is a GUI-based system that uses The Sleuth Kit behind the scenes.

The tools are designed with a modular and plug-in architecture that makes it possible for users to easily incorporate additional functionality. Both tools are free and open-source, but commercial support and training are available as well. [4]

Link for the usage and installation of Autopsy:

- https://medium.com/@tusharcool118/autopsy-tutorial-for-digital-forensics-707ea5d5994d
- https://www.youtube.com/watch?v=g8qAtdFjTwk
- https://www.youtube.com/watch?v=WB4xj8VYotk&t=393s

- **Image creation: FTK imager**

Autopsy and The Sleuth Kit are designed to examine disk images of hard drives, smart phones and so on. The benefit of analyzing an image (rather than a live drive) is that the use of an image allows the investigator to prove that they have not made any modifications to the drive that could affect the forensic results.

Autopsy does not have image creation functionality, so another tool needs to be used. While the majority of the AccessData Forensics Toolkit items are paid tools, its FTK Imager is a free product. This can be used to create disk images that can then be analyzed using Autopsy/The Sleuth Kit. [4]

Link for the usage and installation of FTK imager:

- https://www.hackingarticles.in/comprehensive-guide-on-ftk-imager/
- https://www.youtube.com/watch?v=zDdM7m6YCzA

- **Memory forensics: volatility**

Tools like The Sleuth Kit focus on the hard drive, but this is not the only place where forensic data and artifacts can be stored on a machine.
Volatility is the most well-known and popular tool for analysis of volatile memory. Like The Sleuth Kit, Volatility is free, open-source and supports third-party plugins. In fact, the Volatility Foundation holds an annual contest for users to develop the most useful and innovative extension to the framework. [4]

Link for the usage and installation of Volatility:

- https://resources.infosecinstitute.com/topic/memory-forensics-and-analysis-using-volatility/
- https://www.howtoforge.com/tutorial/how-to-install-and-use-volatility-memory-forensic-tool/

11. Some case studies and concrete examples, e.g. how to carve data from a formatted hard disk as part of the process of a Forensics examination:

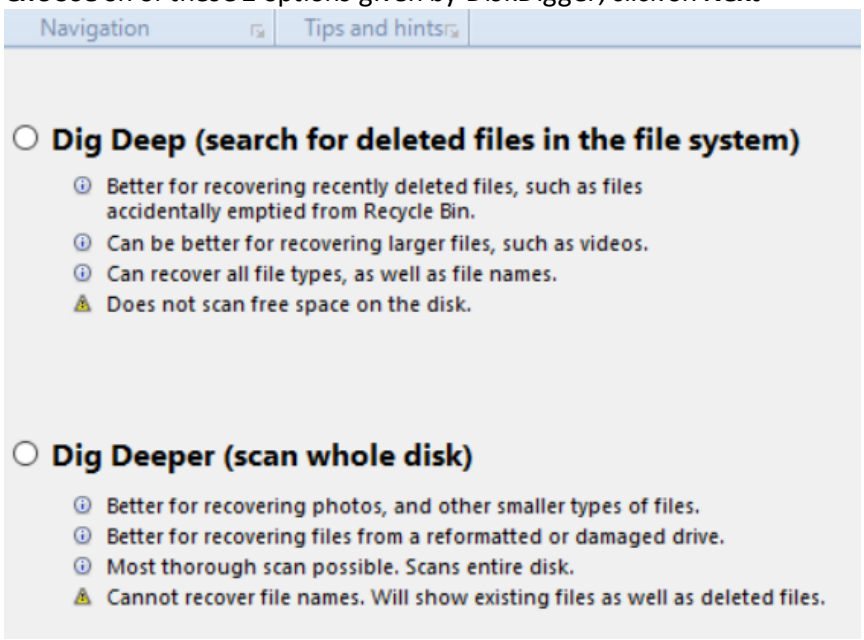
Formatting the hard drive is a bit more secure than simply erasing the files. Formatting a disk does not erase the data on the disk, only the address tables. It makes it much more difficult to recover the files. However a computer specialist would be able to recover most or all the data that was on the disk before the reformat.

File carving is a powerful technique used in computer forensics to extract a formatted file or data from a disk drive or other storage device without the assistance of the filesystem that originally created the file.

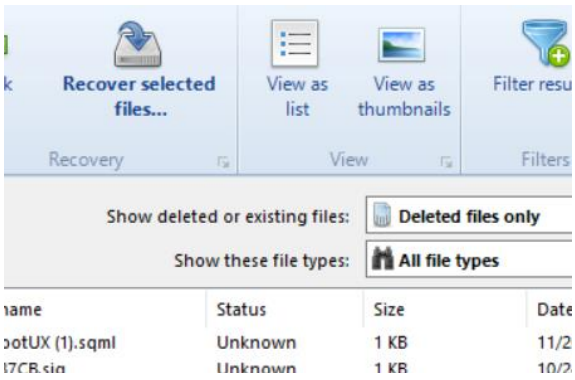
In our example we used the tools Disk Digger and Recuva in order to restored the data. Disk Digger and Recuva are easy and very similar tools to get the data. Recuvo provides more adjustments while restoring the data. But disc digger provides more discriptions to restored data. We have also learnt why data can be restored and what are the restrictions for that. Mainly the data can be restored because of the way the data is deleted and stored in the disc. Recuvo extracts data in a file, while DiskDigger separates them by a file type.

Steps done in order to restore the data from the disk:

1. Install the Disk Digger. The official app can be downloaded from the official web page: https://diskdigger.org/download
2. Connect the device to the application, use mount if needed.
3. Make appropriate adjustments in the **Advanced** section of the DiskDigger
4. **Select** the device from the list of shown on the main page, press on **Next**
5. **Choose** on of these 2 options given by DiskDigger, click on **Next**



6. **Select files** and click on the **Recover the selected files**



7. The files are restored.

References:

[1] John R. Vacca, Computer Forensics, 2nd edition, chapter 1

[2] The laundry. The Laundry. (2021, June 18). Retrieved April 19, 2022, from https://thelaundrynews.com/guidelines-for-digital-forensics-first-responders-best-practices-for-search-and-seizure-of-electronic-and-digital-evidence/

[3] The laundry. The Laundry. (2021, June 18). Retrieved April 19, 2022, from https://thelaundrynews.com/guidelines-for-digital-forensics-first-responders-best-practices-for-search-and-seizure-of-electronic-and-digital-evidence/

[4] 7 best computer forensics tools [updated 2021] - Infosec Resources. (2022). Retrieved 19 April 2022, from https://resources.infosecinstitute.com/topic/7-best-computer-forensics-tools/

[5] The Growing Role of Technology in the Criminal Justice Field. (n.d.). Purdue Global. https://www.purdueglobal.edu/blog/criminal-justice/growing-role-technology-criminal-justice/