Digital Forensics

Tim Schulze

Inhaltsverzeichnis

1 Computer Crime Scene Investigation

1.1 Introduction to Digital Forensics

Computer forensics, also referred to as computer forensic analysis, electronic discovery, electronic evidence discovery, digital discovery, data recovery, data discovery, computer analysis, and computer examination, is the process of methodically examining computer media (hard disks, diskettes, tapes, etc.) for evidence. A thorough analysis by a skilled examiner can result in the reconstruction of the activities of a computer user.
In other words, Computer forensics is the collection, preservation, analysis, and presentation of computer-related evidence.
Computer evidence can be useful in criminal cases, civil disputes, and human resources/employment proceedings. The process of acquiring, examining, and applying digital evidence is crucialto the success of prosecuting a cyber criminal.

- White Color Crimes (health care fraud, government fraud including erroneous IRS and Social Security benefit payments, and financial institution fraud)
- Violent Crimee (child pornography, interstate theft)
- Organized Crime (drug dealing, criminal enterprise)

The objective in computer forensics is to recover, analyze, and present computer-based material in such a way that it is **useable as evidence in a court of law**.
Priority: Accuracy > Speed, but efficiently as possible (adhere to stringent guidelines)

1.2 Roles of Computer in a Crime

A computer can be:

- the target of the crime (audit logs and unfamiliar programs should be checked)
- it can be the instrument of the crime (look for password cracking software and password files)
- it can serve as an evidence repository storing valuable information about the crime

1.3 Computer Forensics Specialist(Procedure sequence)

1. Protect the subject computer system during the forensic examination from any possible alteration, damage, data corruption, or virus introduction

2. Discover all files on the subject system. This includes existing normal files, deleted yet remaining files, hidden files, password-protected files, and encrypted files
3. Recover all (or as much as possible) of discovered deleted files
4. Reveal (to the extent possible) the contents of hidden files as well as temporary or swap files used by both the application programs and the operating system
5. Accesses (if possible and if legally appropriate) the contents of protected or encrypted files
6. Analyze all possibly relevant data found in special areas of a disk
7. Print out an overall analysis of the subject computer system, as well as a 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 computer system examination.
8. Provide expert consultation and/or testimony

1.4 Use of Computer Forensic Evidence

- Criminal Prosecutors(Strafrechtliche Staatsanwälte): homicides, financial fraud, drug and embezzlement record-keeping, and child pornography
- Civil litigations(Zivilrechtliche Streitigkeiten): personal and business records on divorce, discrimination, and harassment cases (Insurance companies)
- Corporations: sexual harassment, embezzlement, theft or misappropriation of trade secrets, and other internal/confidential information
- Law enforcement officials: require assistance in pre-search warrant preparations and post-seizure handling of the computer equipment
- Individuals: hire computer forensics specialists in support of possible claims of wrongful termination, sexual harassment, or age discrimination (electronic mail systems, on network servers, and on individual employee's computers)

1.5 Use of Computer Forensics in Law Enforcement

If there is a computer on the premises of a crime scene, the chances are very good that there is valuable evidence on that computer. If the computer and its contents are examined (even if very briefly) by anyone other than a trained and experienced computer forensics specialist, the usefulness and credibility of that evidence will be tainted.
Make sure you find someone who not only has the expertise and experience, but also the ability to stand up to the scrutiny and pressure of cross-examination.

1.5.1 Employer Safeguard Program

An unfortunate concern today is the possibility that data could be damaged, destroyed, or misappropriated by a discontented individual Before an individual is informed of their termination, a computer forensic specialist should come on-site and create an exact duplicate of the data on the individual's computer. In this way, should the employee choose to do anything to that data before leaving, the employer is protected.

- What Web sites have been visited
- What files have been downloaded
- When files were last accessed
- Of attempts to conceal or destroy evidence
- Of attempts to fabricate evidence
- That the electronic copy of a document can contain text that was removed from the final printed version
- That some fax machines can contain exact duplicates of the last several hundred pages received
- That faxes sent or received via computer may remain on the computer indefinitely
- That email is rapidly becoming the communications medium of choice for businesses
- That people tend to write things in email that they would never consider writing in a memorandum or letter
- That email has been used successfully in criminal cases as well as in civil litigation
- That email is often backed up on tapes that are generally kept for months or years
- That many people keep their financial records, including investments, on computers

1.6 Computer Forensic Services

- Data seizure(Beschlagnahme)
- Data duplication and preservation(Vervielfältigung und Aufbewahrung)
- Data recovery
- Document searches
- Media conversion

- Expert witness services

PROVIDE EXPERT CONSULTATION AND EXPERT WITNESS SERVICES

COMPUTERS

Expert Testimony

- Has testified multiple times as an expert witness in computers and computer forensics in circuit court
- Regularly testify as an expert witness in computers and computer forensics in federal court for U.S. attorney's offices

Computer Expertise

- Belongs to the Computer Crime Investigators Association
- Trained in the forensic examination of computers (PC & Mac), having conducted examinations in countless cases including child exploitation, homicide, militia, software piracy, and fraud
- Has testified in state and federal courts as an expert in computers, computer forensics, the Internet, and America Online; often as an expert witness for U.S. attorney's offices
- Is thoroughly familiar with both computer hardware and software, having written software and repaired and assembled computers
- Teaches computer crime investigation, including computer search and seizure, for the Institute of Police Technology and Management
- Regularly consults with law enforcement officers in the search and seizure of computers
- Has provided forensic training to numerous law enforcement officers and corporate security officers
- Regularly consulted by other forensic examiners for advice in difficult cases

Training Given as Expert in Computer Crimes

- Law Enforcement and Corrections Technology Symposium and Exhibition
- Bureau of Justice Statistics/Justice Research Statistics Association

Electronic Surveillance

- Theft by employees or others
  - Time
  - Property
  - Propriety information and trade secrets
- Embezzlement
- Inappropriate employee actions
- Burglary

Your computer forensics expert's experience should include installing cameras in every imaginable location (indoors and outdoors, offices, homes, warehouses, stores, schools, or vehicles) for every conceivable crime (theft, burglaries, homicides, gambling, narcotics, prostitution, extortion, or embezzlement) under every conceivable circumstance (controlled settings, hostage crisis, or court-ordered covert intrusion).

If you need to know what your employees are doing on your time and on your premises, your computer forensics experts should be able to covertly install video monitoring equipment so that you can protect your interests. This even includes situations where employees may be misusing company computers. By using video surveillance to document employees who are stealing time, property, or secrets from you, you should protect yourself if you plan to take appropriate action against the employees.

Child Exploitation

- Child sexual exploitation
- Child pornography
  - Manufacture
  - Use
  - Sale
  - Trading
  - Collection
  - Child erotica
- Use of computers in child exploitation
- Search and seizure
- Victim acquisition
- Behavior of preferential and situational offenders
- Investigation
  - Proactive
  - Reactive [4]

- Computer evidence service options
  - Standard service
  - On-site service
  - Emergency service
  - Priority service
  - Weekend service
- Other miscellaneous services
  - 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

1.7 Problems with Computer Forensic Evidence

Computer evidence is like any other evidence. It must be:

- Authentic
- Accurate
- Complete
- Convincing to juries
- In conformity with common law and legislative rules (i.e., admissible)

There are also special problems:

- Computer data changes moment by moment.
- Computer data is invisible to the human eye; it can only be viewed indirectly after appropriate procedures.
- The process of collecting computer data may change it—in significant ways. The processes of opening a file or printing it out are not always neutral.

- Computer and telecommunications technologies are always changing so that forensic processes can seldom be fixed for very long [5].

1.8 The Forensic Technican

standard disk repair, network testing

- The scene of crime has to be frozen; that is, the evidence has to be collected as early as possible and without any contamination.
- There must be continuity of evidence, sometimes known as chain of custody; that is, it must be possible to account for all that has happened to the exhibit between its original collection and its appearance in court, preferably unaltered.
- All procedures used in examination should be auditable; that is, a suitably qualified independent expert appointed by the other side in a case should be able to track all the investigations carried out by the prosecution's experts [5].

Key features

- Careful methodology of approach, including record keeping
- A sound knowledge of computing, particularly in any specialist areas claimed
- A sound knowledge of the law of evidence
- A sound knowledge of legal procedures
- Access to and skill in the use of appropriate utilities [5]

1.9 Subject Matter of Computer Forensics

- Authenticity: Does the material come from where it purports?
- Reliability: Can the substance of the story the material tells be believed and is it consistent? In the case of computer-derived material, are there reasons for doubting the correct working of the computer?
- Completeness: Is the story that the material purports to tell complete? Are there other stories that the material also tells that might have a bearing on the legal dispute or hearing
- Freedom from interference and contamination: Are these levels acceptable as a result of forensic investigation and other post-event handling?

1.10 Questions

1. Why are information systems ("computer at crime sites") significant for law enforcement and criminal prosecution? Information systems, including computers, smartphones, and other digital devices, are significant for law enforcement and criminal prosecution because they contain a wealth of information that can be used as evidence in court. Digital evidence can include emails, text messages, social media posts, images, videos, and other types of data that can help investigators build a case against a suspect.

2. What is the meaning of the term digital crime scene? The term "digital crime scene" refers to any situation in which digital devices or systems are involved in a crime. This can include hacking, identity theft, cyberbullying, and other types of offenses that are facilitated by technology. A computer can play one of three roles in a computer crime. A computer can be the target of the crime, it can be the instrument of the crime, or it can serve as evidence repository storing valuable information about the crime.

3. What are the main targets of Digital Forensics? The main targets of Digital Forensics are the data and digital devices that are involved in a crime. This includes computers, smartphones, tablets, and other digital devices that may contain evidence of a crime.

4. What are the main aspects of Digital Forensics? The main aspects of Digital Forensics include the collection, preservation, analysis, and presentation of digital evidence. Digital Forensics experts must use specialized tools and techniques to extract data from digital devices and analyze it in a forensically sound manner.

5. What is the relationship between of Digital Forensics and the classical Forensics? The relationship between Digital Forensics and classical Forensics is that they both involve the use of scientific techniques to collect and analyze evidence. However, Digital Forensics is focused specifically on digital devices and data, while classical Forensics may involve physical evidence such as fingerprints, DNA, and other types of material evidence.

6. What is the general procedure (course of action) of a Digital Forensics examination? Compare the procedure with that of a classical Forensic examination! The general procedure for a Digital Forensics examination involves the collection and preservation of digital evidence, followed by the analysis and interpretation of that evidence. This may involve the use of specialized tools and techniques, such as forensic imaging, data recovery, and malware analysis. The procedure for a classical Forensic examination may involve collecting physical evidence, analyzing it in a laboratory, and presenting the findings in court.

7. Which laws are relevant for a Forensics expert? How to ensure that a Forensics examination is compliant to all relevant laws? Forensics experts must be familiar

with relevant laws related to evidence collection and analysis, such as the Federal Rules of Evidence and the Computer Fraud and Abuse Act. They must also ensure that their examinations are compliant with applicable laws and regulations, such as those related to privacy and data protection.

8. What are typical Forensics tools, a Digital Forensics expert applies during an examination? Compare the tools with those of a classical Forensic examination!

9. What are the main skills and competences, Forensics experts need? (Which of them do you already have / will you have after the lecture?) Forensics experts may use a range of tools and software to assist with digital evidence collection and analysis, such as forensic imaging software, data recovery tools, and malware analysis tools. Classical Forensic experts may use tools such as microscopes, chemical analysis equipment, and fingerprint analysis tools.

10. What kind of services are offered by professional Forensics experts? Forensics experts need a range of skills and competencies, including knowledge of computer systems and networks, proficiency in data analysis and interpretation, and the ability to communicate complex technical information to non-technical audiences. They must also have strong attention to detail and the ability to work well under pressure. Professional Forensics experts may offer a range of services, including digital evidence collection, analysis and interpretation, expert witness testimony, and consulting services to help organizations develop forensic readiness plans.

11. What kind of documents are generated by Forensics experts during an examination? Give names and describe the main contents! Forensics experts may generate a range of documents during an examination, including reports detailing the findings of their analysis, affidavits or declarations describing their methodology and conclusions, and other legal documents required for court proceedings.

12. What are the main problems, challenges, and limitations of a Forensics examination? The main problems, challenges, and limitations of a Forensics examination can include issues related to data acquisition and preservation, data integrity, and the interpretation of complex data. In addition, Forensics experts may face challenges related to changing technology and evolving legal and regulatory frameworks.

13. What is the meaning of the term "Forensics Readiness"? What to do to achieve it?

    "Forensics Readiness" refers to the ability of an organization to prepare for and respond to digital incidents or data breaches in a forensically sound manner. To achieve Forensics Readiness, organizations must develop policies and procedures for incident response and data preservation, and ensure

2 File Carving

Tim Lanzinger, Tim Schulze

2.1 Main goal and role of recovering lost files / meta data

The main goal of digital forensics is to uncover and investigate digital evidence related to cybercrime or other computer-related incidents. This can involve the analysis of computer systems, networks, digital devices, and data storage media to collect and analyze digital evidence.

File carving is a typical example of the work of a digital forensics expert. It involves the extraction of data from a file or storage media that has been damaged, corrupted, or intentionally deleted. File carving uses specialized software tools to search for and extract individual files or fragments of files from the raw data on a storage device, even if they have been partially overwritten or are otherwise inaccessible through conventional methods.

Recovering lost files is an essential part of digital forensics investigations. In many cases, digital evidence may be intentionally deleted or hidden by an attacker or suspect. Recovering lost files can provide valuable evidence for identifying the perpetrator or understanding the sequence of events leading up to an incident. Forensic experts may use a variety of techniques, including file carving, to recover lost files.

Metadata, such as creation date, last modification date, and location data, can also play an important role in digital forensics investigations. This information can help investigators to determine when a file was created, modified, or accessed, and can provide insight into the activities of the user or device in question. Location data, such as GPS coordinates contained in image files, can also provide important contextual information about a crime scene or the movements of a suspect. Forensic experts carefully analyze metadata to build a comprehensive timeline of events and reconstruct the sequence of digital activity related to a case.

2.2 Directory Table and FAT

In a FAT (File Allocation Table) file system, the directory table and file allocation table (FAT) are critical components that keep track of the files and their location on the storage media.

a) After a file is deleted from a FAT file system, the directory entry for the file is marked as deleted, but the actual data for the file may still be present on the disk until it is overwritten by new data. The FAT entry for the deleted file is also marked as available, indicating that the clusters previously allocated to the file are now free for reuse.

b) When a FAT file system is re-formatted using quick formatting, the directory table and FAT are recreated, and all existing data is erased. Quick formatting only deletes the directory table and FAT, but does not overwrite the actual data on the disk. Therefore, the data from the previous files may still be recoverable using data recovery tools until it is overwritten by new data.
After the re-formatting, the directory table and the FAT will appear as if they are blank or initialized with all entries marked as available for use. This can cause problems for data recovery since there may not be any metadata available to indicate the original file names, locations, and sizes. In addition, the quick format does not check for bad sectors, so any existing bad sectors will remain unmarked and could cause problems in the future.

2.3 How file carving recovers

File carving is a technique used by digital forensic experts to recover deleted files or lost data from a storage media. In the case of a FAT file system, file carving can be used to recover deleted files from the clusters that were previously allocated to them in the file allocation table (FAT).

a) When a file is deleted from a FAT file system, the clusters that were previously allocated to it are marked as available for reuse, but the actual data may still exist on the disk until it is overwritten by new data. File carving software can scan the disk for these clusters and try to reconstruct the original file based on the available data fragments. The software looks for the headers and footers of file types, such as .docx, .pdf, .jpg, etc., and reconstructs the file based on the fragments that are found.

b) When a FAT file system is re-formatted using quick formatting, the directory table and FAT are recreated, and all existing data is erased. However, file carving can still be used to recover deleted files in this scenario if the data has not been overwritten by new data. The software scans the disk for the data fragments that belong to the file type being recovered and attempts to piece them together into a recognizable file. The recovered file may not have its original name or file attributes, but the content should still be intact.

2.4 Why you cannot expect file carving to recover all lost files

File carving is a powerful technique used to recover deleted or lost files from a storage device. However, in practice, it is not always possible to recover all the lost files using

file carving. This is because of several reasons such as fragmentation, partial overwriting, defective sectors, quick formatting, and deep formatting.

- Fragmentation: When a file is saved to a storage device, it may be fragmented, i.e., it may be saved in several non-contiguous locations on the disk. In such a case, file carving may only be able to recover parts of the file, but not the entire file.
- Partial overwriting: If a file is deleted, but some parts of it are overwritten by new data, file carving may only be able to recover the remaining parts of the file, but not the overwritten parts. This can result in an incomplete or corrupted file.
- Defective sectors: If there are defective sectors on the storage device, file carving may not be able to recover the data stored in those sectors, resulting in an incomplete or corrupted file.
- Quick formatting: Quick formatting does not actually erase the data on the storage device, but only deletes the file system structures. If the storage device is subsequently used to store new data, the new data may overwrite the old data, making it impossible to recover.
- Deep formatting: Deep formatting erases all the data on the storage device, including the file system structures. In such a case, file carving may not be able to recover any of the lost data.

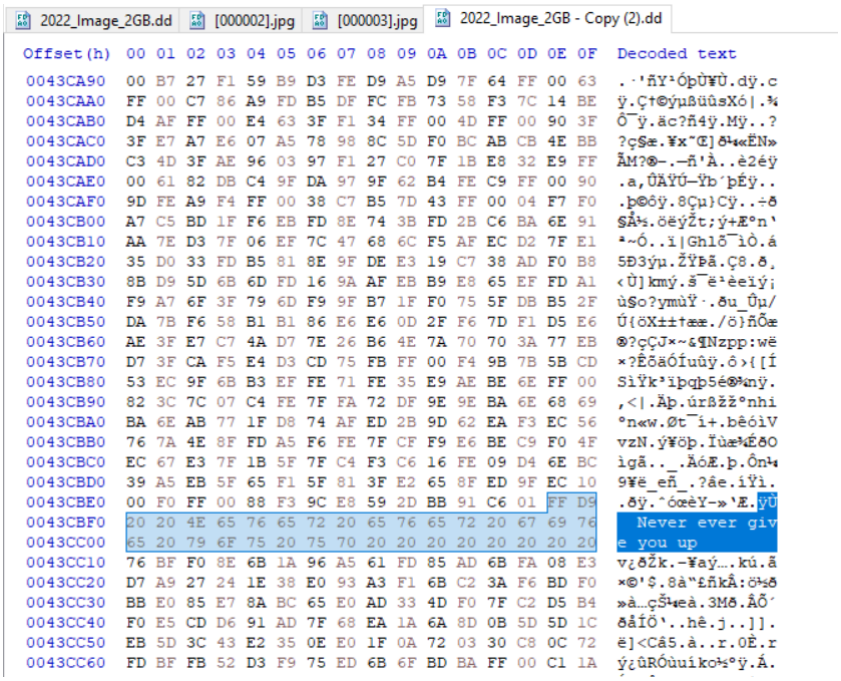
In summary, file carving is a powerful technique, but it has its limitations. The success of file carving depends on several factors, including the extent of data loss or damage, the fragmentation of files, the presence of defective sectors, and the type of formatting used. Therefore, it is important to use file carving in combination with other data recovery techniques to maximize the chances of successful data recovery.

2.5 Labreport

2.5.1 Capture the Flag

First you need to carve for data. For that we used DiskDigger. Now you can Scan the whole Disk(image). You can also use Recuva, for what you need a mounted drive to function.

1. Whats the name of the Captain? Is the being intelligent? .wav-Datei: Name = Jean Luce Picard. Being is intelligent
2. What would Ricky never do? Never ever give you up. Viewed file with HxD, which allows you to see the file jpg in end marker(FFD9).



3. After an Xtensive search, you need to find out which key has a creation date. Name the creation date and the corresponding key! Unsure about solution.

4. Someone shot the shark! What type of Canon did he use? He used a Canon EOS 20D. This is from the Meta-Information from the image, extracted with ExifTool.

5. Theres a famous broom hidden inside of all this mess and he has a message for us! What font did she use to type this message? the message? Was it all a test? Extracted from Powerpoint-File: Font = Nimbus Roman 9L, but it was shown as "Times New Roman", because this is the default font. Message = "I AM A PRETTY GIRL". The headline says that it is a test.

6. Someone is riding on something, what a cool video! Whats his name and on what is he riding? His name is Joe and he is riding a surfboard. (Seen in the .wmv-File)

7. How many observations were necessary to proof, that he excels at it? Extracted from the Excel-File: There were 10 observations.

8. Theres science in there! Whats the title and who wrote it (2 scientists)? Extracted from PDF: Title = "Prudent Engineering Practice for Cryptographic Protocols", Authors = Martin Abadi, Roger Needham.

9. More science! Whats the first name of this good man and the rest of his fellow scientists (3 scientists)? "Joshua", "Jonathan", "F. Javier"

2.6 Discussion

We used two different file carving tools, which there are "DiskDigger" and "Recuva". DiskDigger can carve any files, but Recuva needs a mounted Harddrive to be able to scan it. DiskDigger was also not able to find a deleted file, but Recuva did.

2.7 Summary

In this meeting, we discussed digital forensics, file carving, and the limitations of file carving in recovering lost files from a storage device.
We started by discussing the main goal of digital forensics and how file carving is a typical example of the work of a forensic expert. We also talked about the role of recovering lost files and the importance of metadata, such as creation date, last modification date, and GPS coordinates, in digital forensics investigations.
Next, we discussed how the directory table and file allocation table in a FAT file system look like after a file is deleted and after the file system is reformatted. We learned that file carving can be used to recover deleted files by scanning the disk for data fragments and reconstructing the file based on the available data.
Finally, we discussed the limitations of file carving, such as the effects of fragmentation, partial overwriting, defective sectors, quick formatting, and deep formatting on the success of data recovery. We learned that file carving is not always successful in recovering lost files, and it is important to use other data recovery techniques in combination with file carving to maximize the chances of successful data recovery.

Personal opinion: Files which seem to be lost, are not always lost. They can still be restored, even if small portions of them have been overwritten with other data. JPG-files with an artificially placed end marker (FF D9) can be recovered, and even if a small portion of the image has been overwritten, the image can be recovered with some color distortions (See screenshot). A device, which seemingly has been destroyed, can still have data extracted from it. If I ever find myself in a situation, where I have to recover data which has been deleted or overwritten, I now know which tools to use and how to restore valuable data.

3 Legal Restrictions

Tim Lanzinger, Tim Schulze

3.1 Introduction

The knowledge of legal framework is essential for digital forensics (DF) as it ensures that forensic examiners comply with legal restrictions when performing examinations. Failure to comply with these legal restrictions can result in evidence being deemed inadmissible in court, which could potentially jeopardize the outcome of a case. Furthermore, digital forensic experts need to know about crimes that could be committed to identify relevant digital evidence.

One of the most important legal restrictions applicable to forensic examinations is the admissibility of evidence. Digital evidence must meet certain legal requirements to be admissible in court, including the Frye and Daubert standards. Additionally, the chain of custody must be properly documented and maintained to preserve the integrity of the evidence.

Another important legal restriction is search and seizure. Digital forensic experts must follow proper procedures when conducting searches and seizures to ensure that the evidence obtained is admissible in court. This includes obtaining proper warrants and ensuring that the search is conducted within the scope of the warrant.

To comply with the legal framework in practice, digital forensic experts should document all procedures and steps taken during the examination process. This includes documenting the chain of custody, the tools and techniques used, and any other relevant information related to the examination. Digital forensic experts should also obtain informed consent from the owner or custodian of the digital device or storage media.

A contract between the digital forensic expert and the client is also essential to ensure that both parties understand their rights and obligations. The contract should include the scope of the examination, the fees, and the responsibilities of each party. The contract should also include provisions related to confidentiality and the handling of sensitive information.

In summary, compliance with legal restrictions is essential in digital forensics, and failure to comply can result in evidence being deemed inadmissible in court. Proper

documentation, informed consent, and contractual agreements are important tools for ensuring compliance and protecting the rights of all parties involved.

3.2 Overview of Relevant Laws

3.2.1 Criminal Code

The criminal code outlines laws related to illegal activities, such as theft, fraud, and hacking. Digital forensic experts need to be aware of these laws to identify relevant evidence and ensure that they are not violating any laws themselves during the examination process.

3.2.2 Corporate Law

Corporate law outlines the legal requirements for businesses and organizations. Digital forensic experts may be called upon to investigate corporate fraud or other illegal activities within a company. Understanding corporate law is essential for identifying relevant evidence and ensuring that the investigation complies with legal requirements.

3.2.3 Personal Rights

Personal rights laws protect individuals from invasion of privacy and other violations. Digital forensic experts must be aware of these laws to ensure that their examination procedures do not violate the privacy rights of individuals.

3.2.4 Intellectual Property

Intellectual property laws protect the rights of creators and owners of intellectual property, such as patents, trademarks, and copyrights. Digital forensic experts may be called upon to investigate cases related to intellectual property theft, and they must be familiar with these laws to identify relevant evidence and ensure that the investigation complies with legal requirements.

3.2.5 Copyright

Copyright laws protect the rights of creators and owners of original works, such as books, music, and movies. Digital forensic experts may be called upon to investigate cases related to copyright infringement, and they must be familiar with these laws to identify relevant evidence and ensure that the investigation complies with legal requirements.

3.2.6 Privacy and Data Protection

Privacy and data protection laws regulate the collection, use, and storage of personal data. Digital forensic experts must be aware of these laws to ensure that the examination procedures comply with legal requirements and do not violate the privacy rights of individuals.

In summary, digital forensic experts need to be familiar with a variety of laws and legal requirements related to their work. Each of these laws and standards plays an important role in ensuring that forensic examinations are conducted ethically and legally. By understanding these laws and standards, digital forensic experts can identify relevant evidence, comply with legal requirements, and protect the rights of all parties involved.

3.3 Risk and Considerations in DF Examinations

In this section, we will discuss the potential risks and considerations that DF experts should be aware of when conducting examinations. One important aspect to consider is the risk of infringing on laws while collecting and analyzing data. DF experts must be aware of the legal restrictions and must avoid any actions that may violate them.

Two specific actions that should be avoided are making IT systems or data unavailable (denial-of-service) and modifying data. Both of these actions can reduce the availability of the data and destroy potential evidence. It is important for DF experts to follow the correct procedures for collecting and analyzing data to ensure that the evidence is preserved and admissible in court.

In summary, DF experts should be aware of the potential risks and legal restrictions when conducting examinations. They must adhere to the correct procedures and avoid any actions that may infringe on the law or destroy evidence.

3.4 DF and ISO27k

Digital Forensics (DF) experts can benefit from implementing the guidelines and best practices outlined in the ISO 27000 series of standards, which provide a comprehensive framework for information security management. By using these standards, DF experts can ensure that they are following industry best practices for protecting sensitive information and conducting investigations in a secure and reliable manner.

ISO 27001 provides a framework for implementing an Information Security Management System (ISMS), which includes policies, procedures, and controls for managing sensitive information. DF experts can use this standard to ensure that they are following best practices and guidelines for conducting investigations while protecting sensitive information.

One of the best practices due to ISMS is to improve the log level, store logs safely, and support the reporting of logs. This can be achieved by implementing security controls, monitoring and controlling access to data, and conducting regular risk assessments.

DF experts can also benefit from other ISO 27000 standards such as ISO 27002, which

provides guidelines for information security management, and ISO 27035, which provides a framework for incident management. These standards can help DF experts to implement best practices for protecting sensitive information and responding to incidents during investigations.

In summary, implementing the guidelines and best practices outlined in the ISO 27000 series of standards can help DF experts to conduct investigations in a secure and reliable manner while protecting sensitive information.

3.5 Impacts and resulting measurements

DF experts must ensure that they are complying with all applicable laws and regulations when performing forensic examinations. This includes obtaining written permission from the owner of the IT system or data to be examined, as well as ensuring that the security and privacy of any data obtained during the examination is protected.

One important measure that should be taken is to have a written contract in place with the owner of the IT system or data that outlines the permissions and limitations of the examination. The contract should contain specific language related to the relevant laws and regulations, such as the Criminal Code and GDPR. For example, the contract should include language that ensures compliance with Section 203 of the Criminal Code, which prohibits the unauthorized disclosure of confidential information, and Section 32 of the GDPR, which mandates the use of appropriate security measures when processing personal data.

DF experts must also be aware of the limitations of their authority and never attempt to hack into systems without prior permission. This includes cracking passwords or using other hacking tools to bypass access controls. Additionally, DF experts must never harm the availability of IT systems or data during the examination process.

When performing forensic examinations, it is important to always work on images of the IT system or data if applicable. This ensures that the original data is preserved and protected, and any examination or analysis is conducted on a copy of the data.

Finally, DF experts must never copy sensitive data for personal use or publish it, even if it is discovered during the examination process. All data obtained during an examination must be kept strictly confidential and only used for the purposes of the examination.

By adhering to these measures, DF experts can ensure that they are complying with all applicable laws and regulations, and that they are conducting forensic examinations in a manner that is ethical and respectful of the rights and privacy of all parties involved.