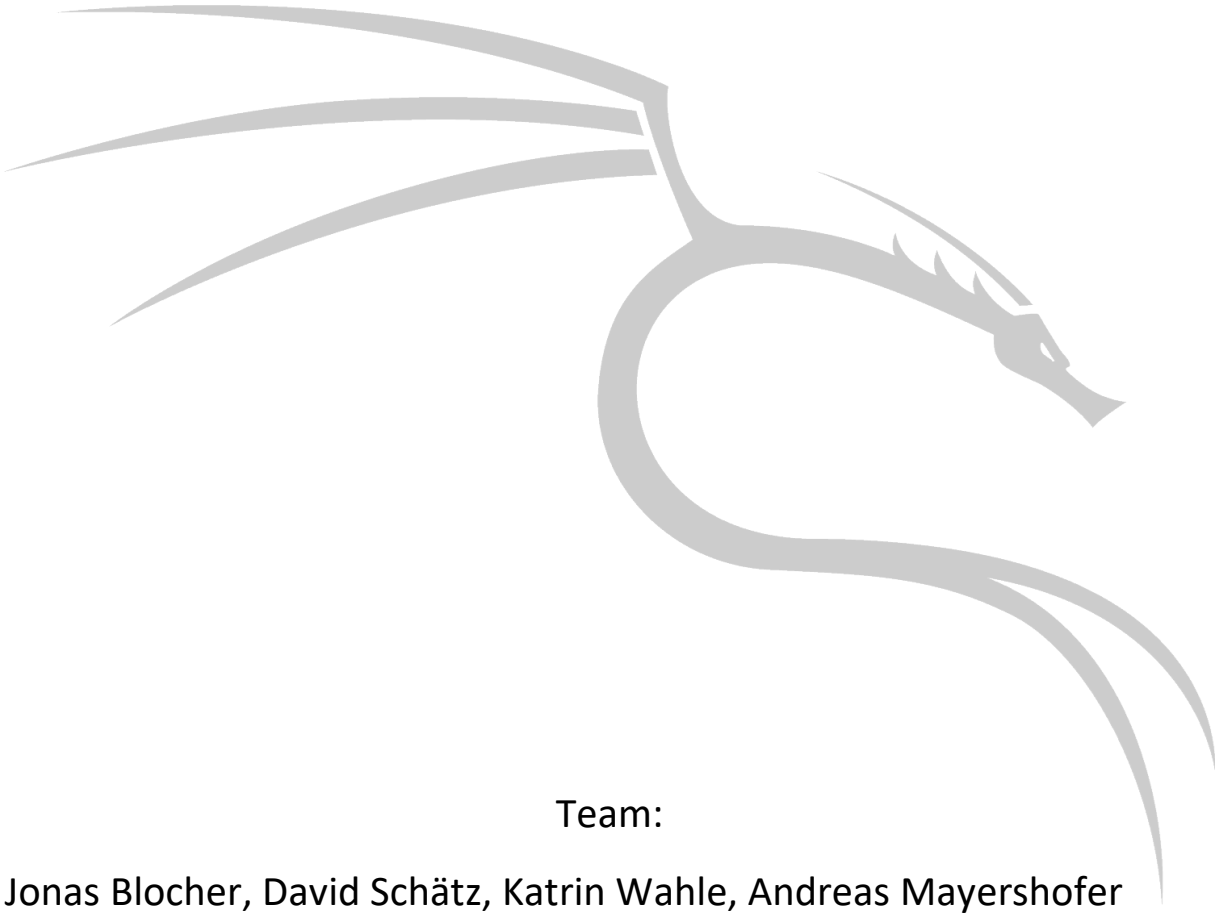
THU
Technische
Hochschule
Ulm

Digital Forensics Handbook



Team:

Jonas Blocher, David Schätz, Katrin Wahle, Andreas Mayershofer

Content

1 Introduction

1.1 Definition of Digital Forensics

In **Classical Forensics** science is applied to gather evidence during an investigation. This includes criminal prosecution but also civil cases. Forensic scientists must collect, preserve and analyze scientific evidence during an investigation, but also testify in court as expert witnesses.
Digital Forensics is a field of forensic science focusing on data found on digital devices. The goal is to uncover or recover data, analyze it, and process it into admissible evidence to present in court.
In DIFO evidential integrity like in classical forensics is of upmost importance.

1.1.1 Differences to classic forensics

Digital forensics and classic forensics have the same aim, namely, to collect evidence. But due to the fact of our digital and networked world, the classic forensics reaches its limits. Therefore, there is digital forensics which take over the search of evidence in the digital world. Of course, the work differs. In the classic forensics you must work with the original objects. The result counts mostly in court. But in digital forensics you work with copies, and you must document every single step you did to prevent suspected manipulation. In the end, the documentation is the more important thing than the result, because the result counts only if you used valid methods.

1.2 A digital crime scene

Any **crime scene** can also be a digital crime scene, if electronic devices were present that could potentially be used or provide **evidence in court**. For a digital crime scene the same rules apply as to any other crime scene: Investigators must make sure to **not destroy or alter any evidence**.
Therefore, first responders should make sure that devices are not turned off or go out of battery. It's a good idea to carry a lockable case with power banks with you. Found devices can be stored there securely and prevented from going out of battery. This is important as when the device is turned off important data in the memory might be lost and any logins turn outdated, locking valuable data behind a password protected encryption.

1.3 Significance of information systems

Information systems are valuable sources for law enforcement as they are likely to store valuable information for the prosecutors. They can be an **instrument** of the crime, the **target** or an **evidence repository**. Even if the data has been corrupted or intentionally deleted Forensics experts can still find evidence. Information systems are used as an interface to access the evidence on the systems in the crime scene. For example, a mobile phone has several valuable sensors.

With the GPS data you can know where a person was, photos show what the Person did, chats show the persons contacts, Bluetooth handshakes represent people, the accused met and so on. This means, that information systems get one of the most important sources in investigations.

1.4 Capabilities of Forensics experts

Forensic Experts do seize Data from devices, duplicate it and preserve it so it can be presented as evidence, recover lost Data, search Documents for evidence, do media conversion and testify a as expert witnesses in courts, to only name a few of their responsibilities.
To do so they must have a meticulous work ethic, including record keeping and have a vast but deep computer science skillset. But they also need knowledge of the law of evidence and of the legal procedures. Of course, they also need to be proficient with the appropriate software tools.
Presentation skills.

1.4.1 Documents

A digital forensics expert provides reasoned answers to questions asked by the person in charge of criminal/court case. It´s important that the report is also readable for no computer experts. The report should contain case details, identifiers, purpose of examination, conclusion, opinions, disposition of evidence.
Also, you must document every single step you did to prevent suspected manipulation (Hash value Checksum shows if data was altered). In the end, the documentation is the more important thing than the result, because the result counts only if you used valid methods.

1.4.2 Challenges

- Evidence must be Authentic, Accurate, Complete, Convincing to juries.
- Computer technology is always changing and is important to adapt to those changes
- Encryption: transforms data to a secured format, unreadable, often covers up important evidence

1.5 Services offered by professional Forensics

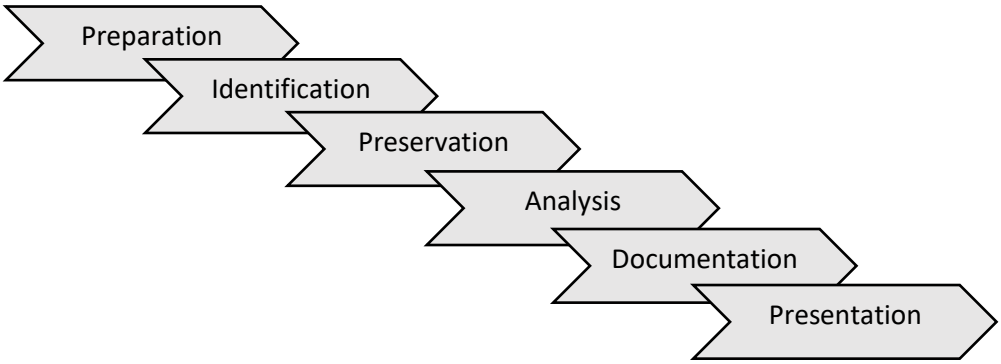
A computer expert should offer different services. The standard service is means, that he works during normal business hours until your issue is resolved. Also, the computer forensics specialist should be able to come to your location to **perform complete computer evidence services**. In a short time, he should **copy all data exactly**, to work with the copy instead of the original. A special point to come to your location is when he **should seize data carriers** on behalf of a court of law. Additionally, an **emergency service should be offered**, which means, that your order has the highest priority, and he doesn’t stop until your evidence objectives are fulfilled.

When the emergency service is too expensive you should be able to choose the Priority Service, which is often twice as fast as the standard service. You can also win time, by booking **the Weekend Service**, so he doesn't stop working on weekend.

1.6 Tools

For different topics, digital forensics experts need different tools. For **File carving** typical software is: Recuva, DiskDigger, foremost. For analyzing **Metadata**, Exif-Tool is a suitable solution. For creating an exact image of a medium, TestDisk is good. To mount such an image, you can use OSFmount. The most famous program for **network analysis** is Wireshark, a software for the analysis and graphical presentation of data logs. For different topics, digital forensics experts need different tools. For File carving typical software is: Recuva, DiskDigger, foremost. For analyzing Metadata, Exif-Tool is a suitable solution. For creating an exact image of a medium, TestDisk is good. To mount such an image, you can use OSFmount. The most famous program for network analysis is Wireshark, a software for the analysis and graphical presentation of data logs. Additionally, the Sleuth Kit is a software collection for the analysis of computer system or a memory image, is necessary for every digital forensics expert. Also, if its really important, file carving in the Hex-editor is also possible. To be able to open found files and document your findings and write reports you also need some kind of office, e.g, Microsoft Office or Libre Office.

1.7 The Forensic examination process



1. **Preparation** of field set: Contract needs to ensure examination is compliant with the law &6 GDPR 201a & STGB
2. **Identification:** Identify Information system with potential evidence on it
3. **Preservation:** Isolate the data by creating an image. Also create a SHA-256 Hash value of the Image to prove it was not altered during the examination process.
4. **Analysis:** Gather, reconstruct data, carve files, and recover as much as possible. This includes existing normal files, deleted yet remaining files, hidden files, password-protected files, and encrypted files. View and analyze the gathered findings and then draw a conclusion based on your findings.

5. **Documentation:** Document every step you during the forensic examination. You can log every command you do in the command line and store it, this way it is very easy to trace back what you did. Also document all your findings, methods, and programs you used.
6. **Presentation:** Present your findings and explain your conclusion.

1.8 Legal aspects of Digital Forensics

Most important: §202a StGB, §6GDPR

1.8.1 Criminal Law

1.8.1.1 §1 StGB No punishment without law

An action taken by someone is only punishable, when at the time of doing the action there is a law in place which states that the action taken is illegal.
An Example of that would be, that if you programmed software which could be used to do data espionage prior to the 26th of November in 2015, where § 202c, which forbids that, was introduced, you could not be punished by that law.

1.8.1.2 §201 StGB Violation of the privacy of the word

Unlawfully either recording private communication or making a recording accessible to a third party without permission may lead to up to three years of jail.

1.8.1.3 §201a Violation of intimate privacy

Taking unauthorized pictures of a helpless individual and/or an individual on their private premises, images with the ability to significantly damage reputations or child pornography and the distribution thereof to a third party can be punished with a fine or up to two years of jail.

1.8.1.4 §202 StGB Violation of privacy of written word

When you think about data espionage in the current age, you think about mostly about it happening in the digital space, but it has its sort of roots in the privacy of written word.
§202 main point is, that you should not open a sealed letter or document not sent to you or try to get any of the informational content of it. Of course, that also applies to digital information as well. Reading postcards is unethical and illegal but will not be punished.

1.8.1.5 §202a Data espionage

Section A further states, that is illegal to work your way around the visible protection that was employed to prevent unauthorized access and if you are not the intended receiver of the digital data and are unauthorized.
An example is data which cannot be read with the eye, e.g. USB drives.
That's why forensic experts always need permission if they try to e.g., carve files out of a formatted HDD. Since the formatting serves as measure to prevent unauthorized access to data.

1.8.1.6 §202b Phishing

Unlawfully intercepting data not intended for oneself from a non-public data processing facility or an electromagnetic broadcast is punishable with a fine or up to 2 years of imprisonment.

1.8.1.7 §202c Acts preparatory to data espionage and phishing

This section states, that even the act of preparing or distributing means to do data espionage like acquiring or developing software which purpose is data espionage or getting a hold on passwords to get access to data is illegal. This even counts software which can be used to do such things, but also has other use cases. (Dual use) These tools could be used for good and for bad purposes.
-> Punishment before committing a crime is possible

1.8.1.8 §202d Handling stolen data

Unless done in a professional manner (taxation/criminal/regulatory offence proceedings), the handling of stolen data for the purpose of enrichment of oneself/a third party is punishable with a fine or up to three years of imprisonment.

1.8.1.9 §203 Violation of private secrets

This section does not apply to computer scientists but does for specialist like doctors or lawyers: business and trade secrets are protected when being told in a professional matter (doctor-patient/attorney-client privilege). Breaking this privilege is punishable with a fine or up to 1 year of imprisonment.

1.8.1.10 §204 Exploitation of secrets of another

The exploitation of secrets related to §203 is punishable with a fine or up to 2 years of imprisonment.

1.8.1.11 §303 StGB Criminal damage

Unlawfully damaging, destroying or altering the appearance of belongings from others is punishable with a fine or imprisonment of up to two years.

1.8.1.12 §303a Data tampering

Someone unlawfully deleting, suppressing, rendering it useless or altering date or even tries to attempt such an act can serve a sentence of up to 2 years.

1.8.1.13 §303b Computer Sabotage

Someone who attacks an IT-System of substantial importance or even attempts to do so can be faced with a sentence of up to 3 years. If it is the system of a business, enterprise or a public authority it may be up to 5 years.

1.8.2 Corporate Law

1.8.2.1 §87 BetrVG Right of co-determination

Workers of a company have the right to co-determine in a variety of matters and as such can organize themselves in a works council. Two of those topics which are especially important to us as forensic experts are first: The matters relating the organization of the enterprise and the behavior of the employees in the enterprise. And secondly: Introduction and use of technical equipment designed to monitor the behavior or performance of employees.
These are of importance for a forensic expert, since it is possible that during an examination done in the company, the examination my reveal data on behavior or performance of employees.
This is why we have to ask the employer for permission before doing the examination, who in turn has to ask the works council for permission.

1.8.2.2 §43 GmbHG(Directors' liability) & §91 AktG(Organization; Accounting)

The Management and Directors who breach their duties are severally and jointly liable to the company for any damages, including information security incidents. The board has to keep the account books maintained and the director must perform risk management.

1.8.3 Personal Rights

1.8.3.1 General data protection regulation

The general data protection regulations (GDPR) main point that anything with personal data is not allowed to be stored. The paragraphs in the GDPR handle, in what cases and under which circumstances and how personal data should be handled.

1.8.3.2 §6 GDPR Lawfulness of processing

This section governs under which circumstances the processing of personal data is lawful and can be summarized in two parts that are important to a forensic expert:

1. Person has given consent to the processing of their personal data.
2. The processing of personal data is necessary to fulfill a contract, comply with a legal obligation or to carry out a task, which is in public interest like presenting digital forensic evidence to court.

1.8.3.3 §25 GDPR Data protection by design and by default

This section of the GDPR states that you should only take personal data you really need and limit it to a minimum. It also states that you should only store it as long as you need and should delete it afterwards.

1.8.4 Standards and Best Practices

1.8.4.1 16.1.1 Responsibilities and procedures

Management responsibilities and procedures need to be established to ensure a fast and effective response to information security and to ensure the forensic readiness

Guidelines for management responsibilities and procedures:

- Procedure for incident response planning and preparation
- Reported information security events and incidents need to be monitored detected and analyzed
- Procedures concerning handling and working with forensic evidence
- Ways of recovery from incidents and communication (internal and external)
- Procedures for assessment of and decision on information security events and information security weaknesses.

To ensure that:

- ► competent personnel handle the information security incidents
- ► a well know interface and contact for security incidents, detection and reporting is implemented

Other Best Practices:

A.16 Information security incident management		
A.16.1 Management of information security incidents and improvements		
Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.		
A.16.1.1	Responsibilities and procedures	Control: Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.
A.16.1.2	Reporting information security events	Control: Information security events shall be reported through appropriate management channels as quickly as possible.
A.16.1.3	Reporting information security weaknesses	Control: Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.
A.16.1.4	Assessment of and decision on information security events	Control: Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.
A.16.1.5	Response to information security incidents	Control: Information security incidents shall be responded to in accordance with the documented procedures.
A.16.1.6	Learning from information security incidents	Control: Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.
A.16.1.7	Collection of evidence	Control: The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.

1.9 Contracts between companies and Forensic experts – How to ensure legal compliance

The contract should include which permissions the forensic expert has, e.g., if they must perform file carving, then they should be granted permission.

It should also handle in which scope the export is allowed to work in and happens if he steps outside of his boundaries and what happens to personal data.

- Parties involved: which companies
- Permission to conduct an analysis
- Term of agreement: until when, conditions to terminate prior
- Standard services: payrate for each service
- Framework: response within 48 hours, max. 1100€/day
- Confidential information: how to handle, inform the employees, illegal possessions may be reported to the authorities (e.g., child pornography)
- Acknowledgement of existing conditions: damage prior to examination may exist, afterwards. Is responsibility assumed
- Warranties

- Liability: who is liable upon injury of personnel, damage to property
- Controlling law: which country/state law is in accordance
  - GDPR §6b: The forensic expert has the right to process the personal information to fulfill his contract. The company ensures the compliance with the law.
  - StGB §203: The expert will not take any data home without permission
  - StGB §202a: The forensic expert gets permission to access evidence even when it means, that they must breaking access controls, e.g. cracking passwords or hack into systems
  - Work Councel Agreement: The work councel (a selected group of employees) represents every employee, therefore agreements signed by the work council are applicable for every employee.

1.10 Forensic readiness

Forensic Readiness is having an appropriate level of capability to be able to preserve, collect, protect and analyze digital evidence so that this evidence can be used effectively.

1.10.1 Measure for Forensic Readiness

- Create a: Principal Computer Forensic Activities Checklist
- Analyze the attack vectors and what attacks can happen, minimize attack vectos
- Education and awareness trainings for employees
- Data security: capability to systematically gather potential evidence and securely preserve it (Decide what to log and where its stored)
- -Legal counsel: make sure your digital forensic methods and practices won't result in a legal matter
- Update your policies for information security and forensic Readiness
- Create an Incident Response Team and train them, or hire a digital forensic expert and make a contract with him BEFORE the incident!
- Install Intrusion detection systems, no detection -> no investigation.

1.10.2 What is an Intrusion detection System?

Intrusion detection Systems are either a software or hardware used to automate the process of intrusion detection, which means monitoring all events occurring on a computer system or network and analyzing for sings of potential intrusion. An intrusion is the unauthorized access of said computer or network and therefore §202a because the attacker needs to break access control The hack includes different architectures and different detection methods IDS use and the option to use an IPS an intrusion prevention system which is an IDS but with the possibility to take actions not only alert a human.

There are two main architectures of an IDS, the Host-based IDS which means that the IDS monitors a single computer system and must be installed. It protects from both internal and external threats. And there are the Network-Based IDS which is a hardware, that analyzes all traffic going through the network e.g activities of applications and protocols, high performance is needed to keep up with the big amount of traffic -> or no real-time is possible. And there is a hybrid version
For the detection methods there is the signature-based IDS which uses a database of know attacks to detect attacks and intrusion (good for known attacks), then there is the anomaly-based detection which uses profiles created from the normal behavior of the users, hosts and regular activities. This represents the known trustworthy behavior, the new behavior is compared to these profiles (good for new and unknown attacks). Also there is a hybrid version its better to combine them.
The IPS tell for example the firewall when there is an Intrusion and blocks the source.
IDS and Digital Forensics
IDS are a great source for collecting digital evidence.
IDS can be used to create digital fingerprints of system users, therefore the behavior of an attacker may stick out compared to the user's typical behavior.
During an attack, an IDS enables the system administrator to collect information such as network connections, running processes, open files, system calls and the memory usage. Because the IDS detects the attack and starts logging. This enables forensic scientists to have a starting point for tracing back a crime to the perpetrator. This evidence is applicable in a court of law.
And there is no investigation without a detection!!!

1.11 Personal Forensics field set

For setting up a forensic field set the choice of the OS is very important. Any Linux based OS works the best for the forensic analysis, but Kali-Linux already includes many tools helpful for performing forensic analysis. To set it up, you need any device capable of running it. You can download the ISO file from the official website and set it up in VMWare Workstation. Any kind of VM or a Raspberry Pi would be sufficient as well. The website also provides a tutorial for the setup, including all the requirements for the devices it is to be set up on.

For my personal digital forensic examinations, I find kali-linux installed on the windows subsystem extremely useful. It has a ton of tools and utilities for examinations, but also allows quick switching to Windows & Microsoft office for documenting the findings and writing case studies. The mounted file systems allow quick exporting and easy access for the files. The subsystem can also easily be cleaned up and replaced with a fresh install, if required.
Kali linux can easily be installed in WSL from the Microsoft shop. A full guide on configuring it with Win-Kex (which allows seamless integration of the linux desktop and the windows desktop) can be found under https://www.kali.org/docs/wsl/win-kex/.

For the occasion that an isolated system is required I use kali-linux on a micro sd card with a raspberry pi 4b.

1.11.1 Install Kali Linux on Raspberry PI

The goal of this Hack is, to install Kali Linux on a Raspberry Pi. You must install Kali Linux on a SD Card (lager than 32GB). Therefore, you must download the right kali image. After that, you need a third-party software (balenaEtcher) to flash the image on the micro-SD Card. After that you cans tart the Raspberry and kali should boot When you want to remote control your Raspberry Pi, you should enable SSH. Maybe you must install it first with “sudo apt-get install ssh”. After that you can enable and start SSH with “systemctl enable ssh” and “service ssh start”. Often root access is necessary, there-fore you must enable it in a ssh config file, because by default it is deactivate. Therefore, open the file /etc/ssh/sshd_config change at PermitRootLogin “no” to “yes”.

Programs

- Guymager for Image Creation
- File carving: Magicrescue, Scalpel and scrounge-nfts
- Autopsy: Autopsy is a GUI for “The Sleuth Kit”, a Software collection for Hard Disk analyzing
- Wireshark: Network analyzing tool
- Reporting Tools like Screen recording

→All these Tools are preinstalled and are import for a digital forensics field, to extract deleted data on a hard disk, because these data can be evidence.

2 Case Studys

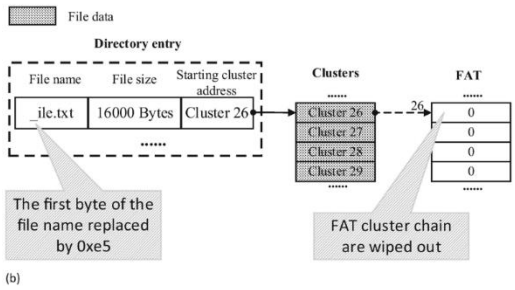
2.1 File carving

2.1.1 Recovering data in a FAT file system

When a file gets deleted in a FAT system, the directory entry is set to a deletion entry(the first byte is set to 0xe5). The file allocation table stays the same, except for the next-cluster-pointers being set to 0x00. As the storage blocks that are occupied by the file are not marked as overwritable, the file continues to use the same disk space as before. All metadata stays preserved. In this case, the file stays recoverable using the OS, a metadata based approach.

When quick-formatting a file system, the directory table gets deleted and the entries in the file allocation table are changed to non-busy. The data on the disk stays the same until being overwritten but the units are marked as unallocated and cannot be recovered using the OS but only by using a file carver.

2.1.1.1 Using metadata



Using this method, the file system scans one directory entry at a time to compile a list of all deletion entries. Then the first byte of all of these entries will be restored (or changed to any legal value). Through the metadata the starting cluster is known. Most files are stored in consecutive clusters, therefore the next-cluster-pointers can be restored easily. This is a very precise way to restore files, but only possible when the data is not fragmented. In an investigation, metadata can be very important. It can be used to rule out suspects by creating alibis. Unfortunately, it can also be tempered with, therefore conclusions drawn by metadata alone might not be reliable.

2.1.1.2 Using a file carver (header/footer carving)

File carvers only use the information stored in data blocks to recover files. Files usually have unique header and footer structures which can be used to reassemble contiguous data blocks. Non contiguous data blocks cannot be recovered automatically and need the forensic expert to remove wrong data blocks. Fragmented content can be recovered often this way.

2.1.2 Reliability of file carving

Even though file carving is a good method to restore files. There are multiple limitations to its functionality. As previously stated, only contiguous data blocks can be recovered reliably. Any fragmentation of the files will make them unrecoverable.

Another problem might occur when previously contiguous data blocks are partially overwritten, turning the recovered file unhelpful. Less frequently, physical damage to the drive, manufacturing defects or wear out can make reads and writes impossible or lead to invalid data as well. Often a single error can affect the entire sector, making it defective.

While deep formatting is, to a limit, able to detect and repair such broken sectors, it may also overwrite files that otherwise would have been carvable.

Other than deep formatting, quick formatting does not detect these errors. But at least it does not alter any of the clusters, except for the file allocation table. Therefore files should be carvable.

2.1.3 Creating a disk image

When performing a forensic analysis it is important that all actions done by the researcher are reproducible. Therefore it is not a good idea to work on the original drive. Instead a disk image should be created and used. This is a file containing the structure and the contents of a partition or

an entire storage device. Usually it is a sector by sector copy of the media. That way it can perfectly mimic the original physical state, independently from the file system.

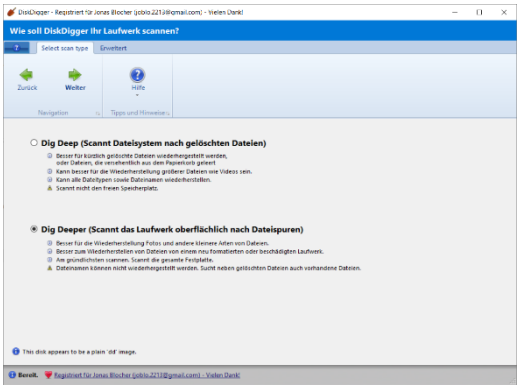
Before connecting the storage medium it should be ensured that auto mounting is disabled. Then it should be mounted manually in read only mode. As this is hardly possible in Windows, it is unsuitable for a proper forensic analysis. For the lab exercise we disabled auto run in the system settings and were careful to not write on the SD card nor to format it.

For creating the disk image testdisk_win was used. On Kali Linux it can easily be done using dd.

2.1.4 File Carving with DiskDigger

DiskDigger allows loading our previously created disk image and carving for lost files.

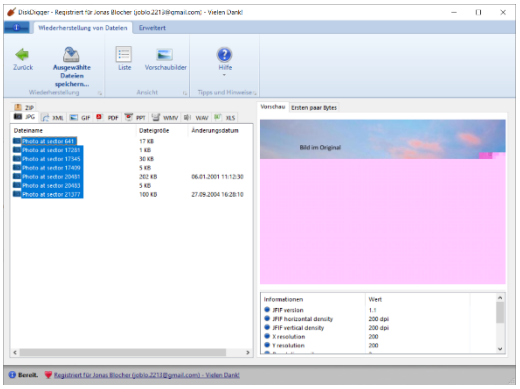
The option is located at “Scan disk image” at “Extended” view.



After selecting the file one of two modes must be chosen:

The “DigDeep” mode searches for deleted files by looking for deletion entries in the directory table that are marked with a special character.

The “DigDeeper” mode performs actual file carving by walking through the clusters of the storage media, scanning for known signatures of file types that indicate lost files. Therefore, the latter mode was chosen.

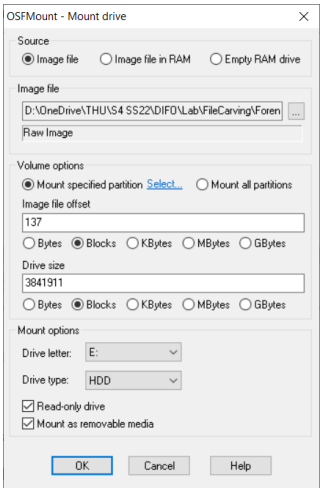


Then the file types that DiskDigger should scan for must be selected.

After processing Diskdigger shows the results, sorted by file type and allows exporting them.

2.1.5 File Carving with Recuva

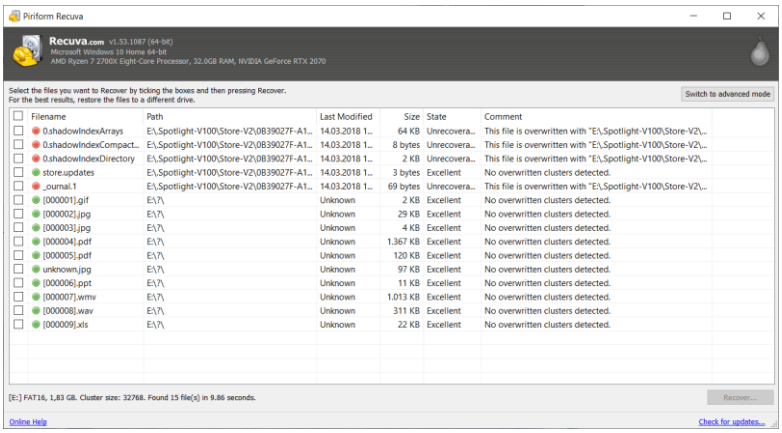
Unfortunately, Recuva only allows scanning mounted volumes. This can be bypassed by using OSFMount to mount the previously created image. It must be made sure to precisely mimic the original storage media properties when configuring the volume.



After mounting the volume, Recuva can be launched. The setup procedure is similar to DiskDigger, but varies in order.First, the file types to recover must be selected. After selecting “All Files”, the previously mounted volume had to be selected as location. To perform file carving

and not just scan the Directory Table for deletion entries “Deep Scan” must be activated.

Recuva shows a list of recoverable and unrecoverable files after running the scan:



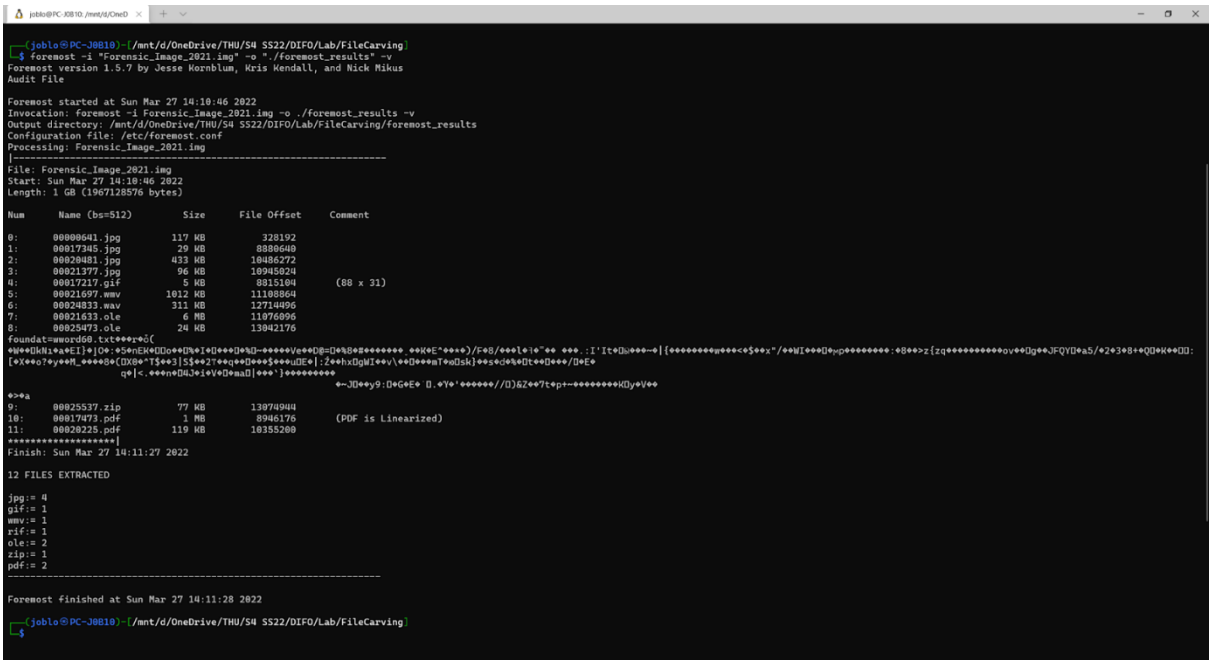
When comparing these results to the files recovered using DiskDigger, it becomes evident that Recuva cannot recover partially overwritten files.

2.1.6 File Carving with Foremost

DiskDigger and Recuva are only available for Windows and not designed for a proper forensic examination. Better suited is Foremost, a tool included in Kali Linux.

It has the additional benefit of creating an audit file that references the parameters used to run it, date, time and a full summary of all findings.

The parameters -i & -o for setting input and output files were used as well as -v to enable verbose output. Use Foremost -h for a full list of available parameters.



Comparing the results to the findings from DiskDigger & Recuva, Foremost was able to recover partially overwritten files. Unfortunately, there were difficulties recognizing files which utilize the Object Linking & Embedding (OLE) technology by Microsoft:

The .ppt and .xls files were found but their file type could not be determined. It is still possible to view them when modifying the extension.

2.1.7 Sources

Lin, X. (2018). Introductory Computer Forensics A Hands-on Practical Approach. Springer.
ISBN: 978-3-030-00580-1

John R. Vacca (2005). Computer Forensics: Computer CrimeScene Investigation. Charles River Media.
ISBN: 978-1-58450-389-7

2.2 AnDercover Challenge

2.2.1 Forensic Tools

To solve the case, you need Wireshark. It doesn't matter if you install it on Windows or Linux, because it is on all platforms the same. With Wireshark you can open the ".pcap" file. The file includes a 254 second recording of network traffic from Ann's laptop. Most of the packets recorded are having the protocol TCP and SMTP. For use only the SMTP Packages are of interest, because SMPT is a protocol that is used to exchange emails in computer networks. That means, such SMPT Packages can contain email messages.

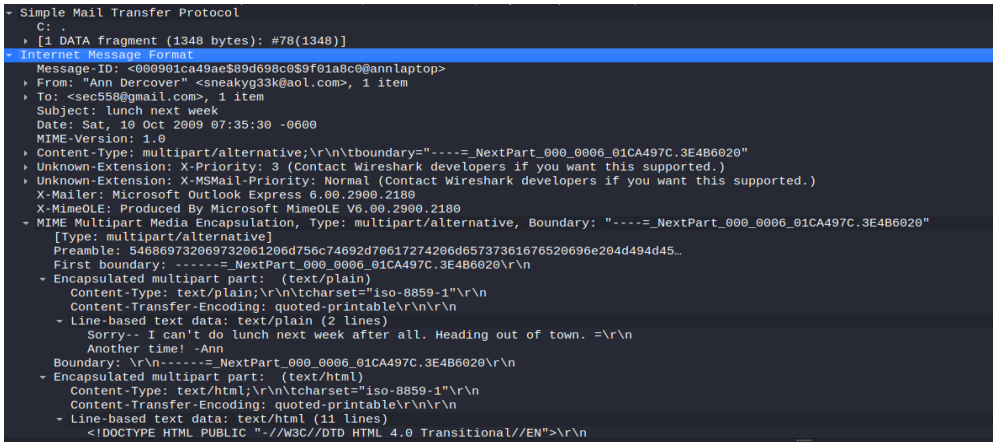
Additionally, we need a base64 decoder. This can be done from the Linux command line - just pipe the base64 encoded string into the base64 -di command. You can use an online tool like https://base64.guru/converter/decode/file.

The decoder is needed because username and passwords are usually encoded with base64 when using the HTTP Basic Authentication. Also, files in the Appendix are encoded in this way.

Furthermore, a text program to open the ".docx" file and an email program such as "Thunderbird", to virtualize the email, can be useful, but is not necessary.

2.2.2 The Emails

In the .pcap log are captured two different mails. One from Ann to his secret lover, and one to another person. The primary message for our interest is the message to her lover.



The first Mail. Which is not interesting for our customer. It is canceling information for a meeting.

```
<DIV><FONT face=3DArial size=3D2>Hi sweetheart! Bring your fake passport =\r\n
and a=20\r\n
bathing suit. Address attached. love, Ann</FONT></DIV></BODY></HTML>\r\n
```

This is the message. Which our client is interested in. The Message is encoded in HTML.

Attached the email one Document -> see below. The Document is encoded in base64. Attachments are mostly encoded in base64 because Smtp can only handle one file per message. So the complete message is in one “file”.

```
▾ Encapsulated multipart part:  (application/octet-stream)
    Content-Type: application/octet-stream;\r\n\tname="secretrendezvous.docx"\r\n
    Content-Transfer-Encoding: base64\r\n
    Content-Disposition: attachment;\r\n\tfilename="secretrendezvous.docx"\r\n\r\n
  ▸ Data (283864 bytes)
```

```
▾ Internet Message Format
    Message-ID: <001101ca49ae$e93e45b0$9f01a8c0@annlaptop>
  ▸ From: "Ann Dercover" <sneakyg33k@aol.com>, 1 item
  ▸ To: <mistersecretx@aol.com>, 1 item
    Subject: rendezvous
    Date: Sat, 10 Oct 2009 07:38:10 -0600
    MIME-Version: 1.0
  ▸ Content-Type: multipart/mixed;\r\n\tboundary="----=_NextPart_000_000D_01CA497C.9DEC1E70"
  ▸ Unknown-Extension: X-Priority: 3 (Contact Wireshark developers if you want this supported.)
  ▸ Unknown-Extension: X-MSMail-Priority: Normal (Contact Wireshark developers if you want this supported.)
    X-Mailer: Microsoft Outlook Express 6.00.2900.2180
    X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.2180
  ▾ MIME Multipart Media Encapsulation, Type: multipart/mixed, Boundary: "----=_NextPart_000_000D_01CA497C.9DEC1E70"
      [Type: multipart/mixed]
      Preamble: 546869732069732061206d756c74692d70617274206d6573736167652069…
      First boundary: ------=_NextPart_000_000D_01CA497C.9DEC1E70\r\n
    ▾ Encapsulated multipart part:  (multipart/alternative)
        Content-Type: multipart/alternative;\r\n\tboundary="----=_NextPart_001_000E_01CA497C.9DEC1E70"\r\n\r\n
      ▾ MIME Multipart Media Encapsulation, Type: multipart/alternative, Boundary: "----=_NextPart_001_000E_01CA497C.9DEC1E70"
          [Type: multipart/alternative]
          Preamble: 0d0a
          First boundary: ------=_NextPart_001_000E_01CA497C.9DEC1E70\r\n
        ▾ Encapsulated multipart part:  (text/plain)
            Content-Type: text/plain;\r\n\tcharset="iso-8859-1"\r\n
            Content-Transfer-Encoding: quoted-printable\r\n\r\n
          ▾ Line-based text data: text/plain (2 lines)
              Hi sweetheart! Bring your fake passport and a bathing suit. Address =\r\n
              attached. love, Ann
          Boundary: \r\n------=_NextPart_001_000E_01CA497C.9DEC1E70\r\n
        ▾ Encapsulated multipart part:  (text/html)
            Content-Type: text/html;\r\n\tcharset="iso-8859-1"\r\n
            Content-Transfer-Encoding: quoted-printable\r\n\r\n
          ▾ Line-based text data: text/html (11 lines)
              <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">\r\n
```

This picture shows the message of our interest.

2.2.3 Solutions of the questions

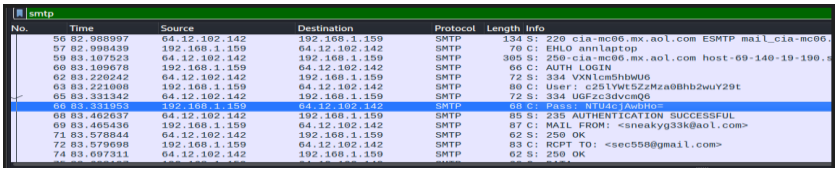
2.2.3.1 What is Ann’s email address?

FROM: <sneakyg33k@aol.com>

2.2.3.2 What is Ann’s email password?

smtp.auth.password=(NTU4cjAwbHo=) 558r00lz

To answer question one and two you need to set the filter in Wireshark to smtp, after that you can see a typical SMTP Authentication-process. directly at the start. In Line 10 you could see the MAIL FROM: but that should not be taken as 100% evidence because it can be faked, so it is less reliable than actually looking at Base64 encoded user authentication, which can be seen from line five to eight. The information is right because there is a 245 AUTHENTICATION SUCCESSFUL answer in line nine.



Here you can see line 5-8, the the encoded text u can see in the tool on the left and the base64 decoded text on the right:

Text: (Base64)	Cleartext
334 VXNlcm5hbWU6	334 Username:
c25lYWt5ZzMza0Bhb2wuY29t	sneakyg33k@aol.com
334 UGFzc3dvcmQ6	334 Password
NTU4cjAwbHo=(Smtp Password)	558r00lz

2.2.3.3 What is Ann's secret lover's email address?

"mistersecretx@aol.com". See in the Header of the DataSection.

2.2.3.4 What two items did Ann tell her secret lover to bring?

"fake passport and bathing suit". This is the visible cleartext out of the DATA segment.

2.2.3.5 What is the NAME of the attachment Ann sent to her secret lover?

"secretrendezvous.docx". Found in the DATA section..

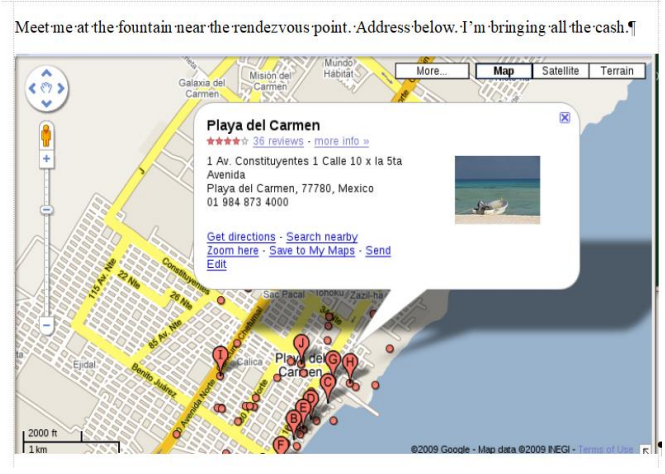
2.2.3.6 What is the MD5sum of the attachment Ann sent to her secret lover?

Secretrendezvous.docx: 9e423e11db88f01bbff81172839e1923

1. Extcrat base64 string -> with the above namend online converter to an .doxc file.
2. The md5sum cann be calculate with the cmd: "md5sum *.docx"

2.2.3.7 In what CITY and COUNTRY is their rendezvous point?

Playa del Carmen, 77780, Mexico. This can be seen when opening the DOCX. As an alternative it is possible to extcrat the .docx. As an Zip file and analyse the file without open it.



3 Hacks

removed