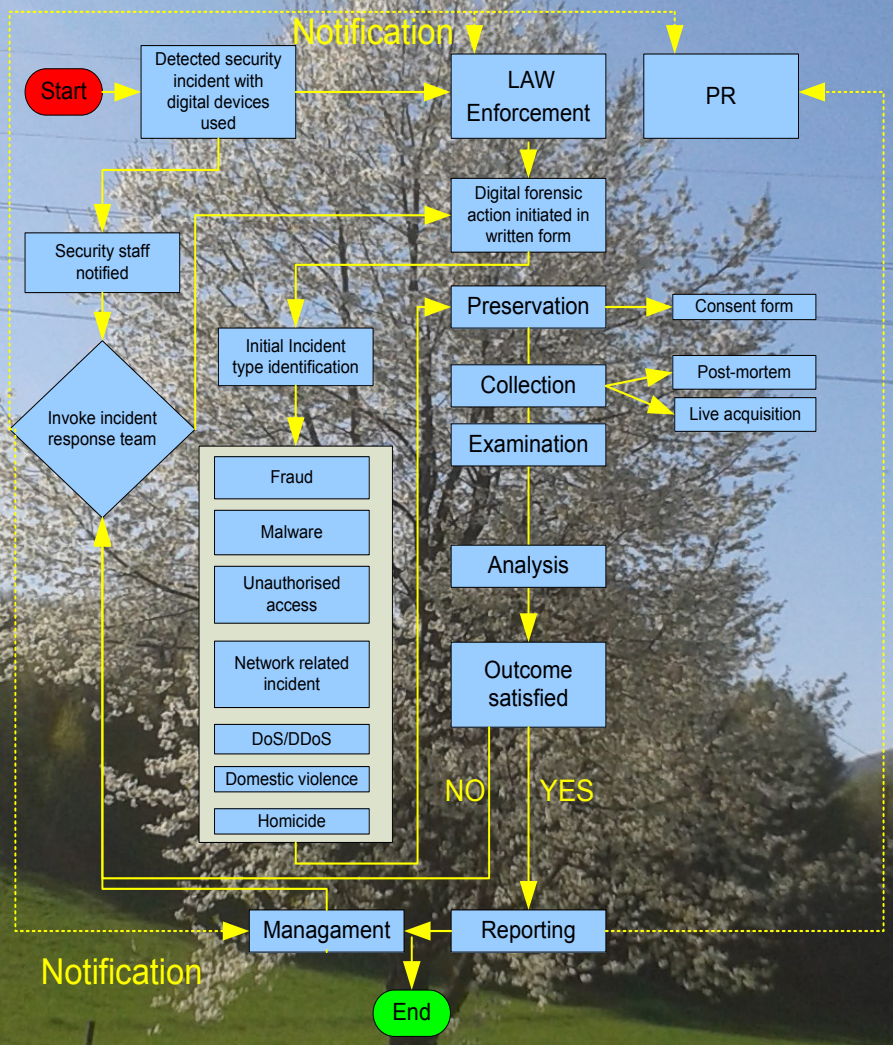
Essentials of Digital Forensics



Kemal Hajdarevic with
Nermin Ziga and Mirza Halilovic

Essentials of Digital Forensics

Kemal Hajdarevic with

Nermin Ziga and Mirza Halilovic

Sarajevo, 2019

Authors:
Dr. Kemal Hajdarevic with Nermin Ziga and Mirza Halilovic

Proofreading: Ana Tankosic

Publisher:
International Burch University

Editor-in-Chief:
Dr. Kemal Hajdarević

Reviewed by: Dr. Hamid Jahankhani, Dr Jasmin Azemovic and Dr. Colin Pattinson

DTP & Design:
Dr. Kemal Hajdarevic

DTP and Prepress:
International Burch University
Circulation: electronic copy

Place of Publication: Sarajevo

CIP - Katalogizacija u publikaciji
Nacionalna i univerzitetska biblioteka
Bosne i Hercegovine, Sarajevo
343.98:004
HAJDAREVIĆ, Kemal
Essentials of digital forensics [Elektronski izvor] / Kemal Hajdarevic, Nermin Ziga, Mirza Halilovic. - El. knjiga. - Sarajevo : International Burch University, 2019
Način pristupa (URL): https://omeka.ibu.edu.ba/items/show/3447. - Nasl. sa nasl. ekrana. - Opis izvora dana 11. 7. 2019.

ISBN 978-9958-834-66-0
1. Žiga, Nermin 2. Halilović, Mirza
COBISS.BH-ID 27750406

Table of Contents

Author's Preface

Information available on Internet Live Stats web site (www.internetlivestats.com) that 40 percent of world's population is using Internet Media almost daily reports on different cyber and digital security incidents. Many more similar incidents have never been reported or they have been reported years after they had occurred due to the fact that they could have jeopardised ongoing law enforcement investigations or because they could have been embarrassing and thus negatively affect reputation of the victim – organisation or a person.

After cyber- or information security incident, the obvious step is to make efforts to minimize losses, establish practices to avoid future similar situations, and punish executioners and/or masterminds of the incident to discourage future attempts.

To be able to accomplish the above-mentioned goals it is necessary to understand the nature of the incident, actual losses, and detect, collect, and preserve evidence, as well as to detect and locate executives of attack that led to the cyber incident.

A common scientific approach of collecting, preserving, analysing, and reporting criminal cases where computers and digital equipment are used

or where they have been an object of the attack is called the digital forensics. If a specific device or software is the object of the forensic investigation process, the scientific approach can be called computer forensics, network forensics, database forensics, etc.

There are different areas of digital forensics based on the object of the criminal activity and on technological tools used to commit an attack.

Digital forensics can be performed by external forensic service or it can be done in a house. Knowledge about forensic process is very important even if the external forensic knowledge or service is used so that affected organisation is able to monitor external forensic service or to perform forensics internally if there are enough internal resources for such an activity.

Some of the first professionals that can detect criminal or fraud activities where computers are involved are computer operators and system or network administrators. Another profession that can have an active role in detecting fraud or abuse of the system resources are internal auditors. Because internal and external auditors have experience, and a broad knowledge of computer and network systems, they can detect criminal activity and perform initial forensic analysis. However, forensics and audit are not the same process, and differences between the two are presented in this book.

Not every organisation is obliged to have a regular internal and external audit, or testing for technical vulnerabilities (also called penetration

testing), nevertheless, from the experience of organisations which have this type of assurance and from incidents which occurred in the past, regular vulnerability checks are needed. Auditors can be given the task by the top management to analyse a fraudulent or a criminal activity as professionals who already have an in-depth knowledge of the specific system. Furthermore, revealing the information about fraud or crime to the public can bring a negative publicity.

That is why it is important for computer professionals, information technology professionals, and internal auditors to understand steps and procedure of the digital forensic investigation process. It is also important for them to understand what a good digital forensic practice should be and what should not be done during the forensic process.

The aim of this book is to clarify forensic topics and bring them closer to students, professionals, information security managers, internal auditors, and other IT specialists who want more information about digital forensic process, tools, and activities. Based on Criminal Justice Degree Schools (2019) as well as courses and authors' experience in teaching, this book also names potential and some already taught courses in computer forensics and information security.

Important definitions

Data - *"factual information (such as measurements or statistics) used as a basis for reasoning, discussion, or calculation,* (Data, Merriam-Webster, 2019)

Information *– "a signal or character (as in a communication system or computer) representing data; the communication or reception of knowledge or intelligence,* (Information, Merriam-Webster, 2019)

Information technology *– "the technology involving the development, maintenance, and use of computer systems, software, and networks for the processing and distribution of data".* (Information technology, Merriam-Webster, 2018).

Information system (IS) *– "an integrated set of components for collecting, storing, and processing data and for providing information, knowledge, and digital products… The main components of information systems are computer hardware and software, telecommunications, databases and data warehouses, human resources, and procedures…",* (Information system, Britanica, 2019)

Information System (IS) Security – "*Refers to the activities, processes, methodologies, frameworks, and standards used for the maintenance of information and information assets confidentiality, integrity, and availability".* (Techopedia, 2018)

Forensics *– "belonging to, used in, or suitable to courts of judicature or to public discussion and debate"* (Forensic, Merriam-Webster, 2018).

Digital forensics - includes not only computers but also any digital device, such as digital cameras, flash drives, digital networks, cell phones, IoT. Wiley C. (2019)

Internal auditing - "*Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.*" (IIA, 2019)

Purpose of this book

The purpose of this book is to provide an insight into forensics of computer and other digital devices. This is because the world of physical operations and business is changing into digital and the world of Internet wherever possible, thus creating a greater risk of cyber-attacks. In common business surroundings, criminal activities are not something that business owners would like to encounter. Considering that digital world and cyber-attacks are not something that business owners usually come in contact with, they are more often not prepared for the aftermath of the potential incident. They are also unaware of their need for the computer or digital forensics investigation process. Thus, the purpose of this book is to familiarize them with the following: Confidentiality, Integrity, Availability (CIA), Authentication, Authentication, and Audits.

Computer Forensics and information Security Training Courses

Following are the courses in the field of information security and cyber forensics:

- Computer Forensics Essentials
- Cybercrime

- Current Issues in Cyberlaw
- Computer Forensics File Systems
- Architecture of Secure Operating Systems
- Forensic Analysis in a Windows Environment
- Forensic Analysis in a Linux/Unix Environment
- Malware and Software Vulnerability Analysis
- Network Security
- Network Forensics
- Mobile Forensics Analysis
- Forensic Management of Digital Evidence
- Cyber Incident Analysis and Response
- Digital Forensics Investigative Techniques
- Forensic Management of Digital Evidence
- Computer Forensic Ethics
- Advanced Topics in Computer Forensics
- Information Systems Security Planning and Audit

Criminal Justice Degree Schools (2019)

Jobs related to computer forensics and information security

Based on Criminal Justice Degree Schools (2019) and authors' experience following are some job titles common in the cyber security industry:

- Business Intelligence Analyst
- Information Security Auditor
- Information System Auditor
- Crime Analyst

- Computer Forensics Investigator
- Computer Systems Analyst
- Cybersecurity Officer
- Digital Forensics Investigator
- Digital Forensics Specialist
- Information Security Officer
- Chief Information Security Officer
- Information Security Analyst

Organisation of the book sections

This book is divided into six sections:

1. Introduction to digital forensics
2. Digital forensics – classification
3. Digital forensics – process
4. Digital forensics – tools
5. Simulation of digital forensic cases
6. Conclusions

While reading, it is possible to follow different tracks.

Learning tracks

It is possible for a reader to acquire a specific set of skills and knowledge on certain paths through different chapters.

Chapter **Job title**	Introduction	Digital forensics classification	Digital forensics process	Digital forensics tools	Digital forensics cases
Business Intelligence Analyst	X	X	X		X
Information Security Auditor	X	X	X		
Information System Auditor	X	X	X		
Crime Analyst	X	X	X	X	X
Computer Forensics Investigator	X	X	X	X	X
Computer Systems Analyst	X	X	X	X	X
Cybersecurity Officer	X	X	X	X	X
Digital Forensics Investigator	X	X	X	X	X
Digital Forensics Specialist	X	X	X	X	X
Information Security Officer	X	X	X		X
Chief Information Security Officer	X	X	X		X
Information Security Analyst	X	X	X	X	X

1. Introduction to digital forensics

Chapter abstract

Chapter goals: Digital transformation has a great impact on cyber forensics because of new services in place, new technologies, and devices. This chapter presents some general information about the early advancements in forensics, and digital forensics. It also provides the explanation of what the digital evidence is and in what state it can be found. Furthermore, this chapter explains different types of digital forensics as well as the difference between digital forensic analysis types. Digital forensics is usually followed by and triggers incident response process which is also explained in this chapter.

Learning outcomes: Learning about one aspect of the forensic history. Knowledge of the core principles of forensics and digital forensics.

History of forensics

In early societies there was a need to resolve different issues and disputes in an acceptable manner so that conclusions are clear and there is no space for ambiguities. As presented in Figure 1. the English word forensic comes from the Latin word *forum* and it initially meant "in open court" (Williams A., 2000).

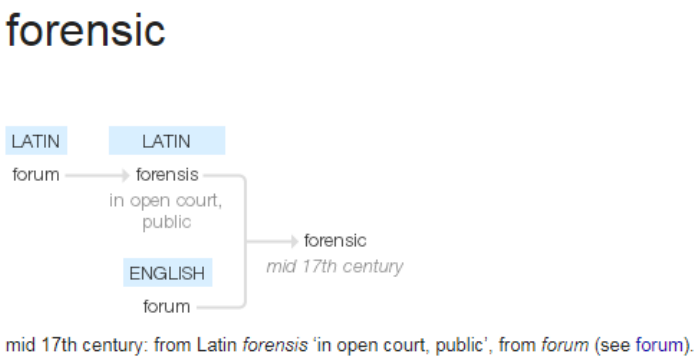


Figure 1. Word "Forensic" explanation (google, 2018)

Historians found evidence of the ancient societies' need for clarification of criminal and other cases in process of finding the truth for the events that happened before, using the science of that time and common knowledge for a better understanding of past events (Williams A., 2000). It was a practice to present evidence to the public for comments and criticism with a goal to make everyone aware of what happened in a specific case. With time, forensic process became a key part of all criminal investigation cases which came later.

Forensic process became a key step of every future criminal investigation case, because every criminal case needed a resolution in terms of finding who is responsible for the wrongdoings.

Edmond Locard Principle of Exchange (Crime Museum, 2019):

> *"..when a person commits a crime something is always left at the scene of the crime that was not present when the person arrived."*

The "*something*" is the goal of every forensic investigator, and it is crucial to detect and preserve it for the later use in the process of reporting findings.

German born scientist Archibald Reiss was the founder of the first academic forensic science program and Institute of forensic science at the University of Lausanne in 1909. (Witte de With, 2019).

Through history, forensics as a discipline is perhaps mostly known from the medical pathology cases, however, recent history shows that traffic accident cases, usage of firearms, and digital and computer equipment also became an important area of forensic investigations.

One view on history of forensics would certainly include usage of fingerprints found at the crime scene. Because of its uniqueness, the fingerprint became an important resource which is used to authenticate each person. As some other scientific advancements, the fingerprint used for the forensic purposes contributed more than a single inventor (History of Fingerprints, 2018). Recent advancements in computer technology use pictures and videos to identify a person with a high accuracy (Kremic, Subasi, Hajdarevic, 2012).

Other important methods used for forensic purposes were blood groupings, and DNA sampling, firearms and bullet comparison, traffic analysis, and other (History of Fingerprints, 2018) as listed below:

- Francis Galton, Edmond Locard – study of fingerprints
- Leone Lattes – Discovered blood groupings (A, B, AB, & 0)

- Calvin Goddard – Firearms and bullet comparison
- Albert Osborn – Developed principles of document examination

Due to different areas where scientific forensics can help in solving disputes, different forensic research areas emerged, some of which are named below:

- Forensic Pathology – Sudden unnatural or violent deaths
- Forensic Anthropology – Identification of human skeletal remains
- Forensic Psychiatry – Forensics of psychiatric cases
- Forensic Odontology – Dental forensics

History of digital forensics

Computers are objects of early forensic investigations, and digital forensics is related to all digital equipment, not only computer devices. Today many digital devices that use, store, and communicate digital data are available. All these digital devices are potential candidates for forensic investigation cases.

Below is a short history of digital forensic advancements:

- 1984 FBI Computer Analysis and Response Team (CART) was formed.
- 1991 International Law Enforcement meeting was held to discuss computer forensics and the need for the standardized approach.
- 1997 Scientific Working Group on Digital Evidence (SWGDE) was established to develop standards.
- 2001 Digital Forensic Research Workshop (DFRWS) was established for development of the research roadmap.

Digital forensics – definition

Digital forensic investigators use science throughout the entire process of collecting, analysing, and reporting evidence.

Digital Forensic Science (DFS) is defined by Digital Forensic Research Workshop (DFRWS, 2001) as:

> *"The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations."*

Digital evidence

Heart of every digital forensic investigation is data as evidence upon which the entire potential case is built. When considering types of digital forensics, one approach could be to classify digital forensic analysis based on data sources for digital investigation, because data is crucial for making decisions, navigating through evidence, and producing the digital forensics report.

Digital vs. Computer forensics

Digital evidence is the heart of every digital forensic investigation and sometimes the term computer forensics is used to refer to the same process. Computer forensics is related to the forensics of computers and related devices, as well as associated software used on computers. On the other hand, digital forensics has a wider scope which includes digital devices such as smart and cell phones, flash drives, media devices, and digital cameras. The purpose of digital forensics is to determine whether a device is used in a criminal act. Criminal act can be the computer fraud, computer hacking, traffic accidents, illegal pornography distribution, etc. Wiley C. (2019)

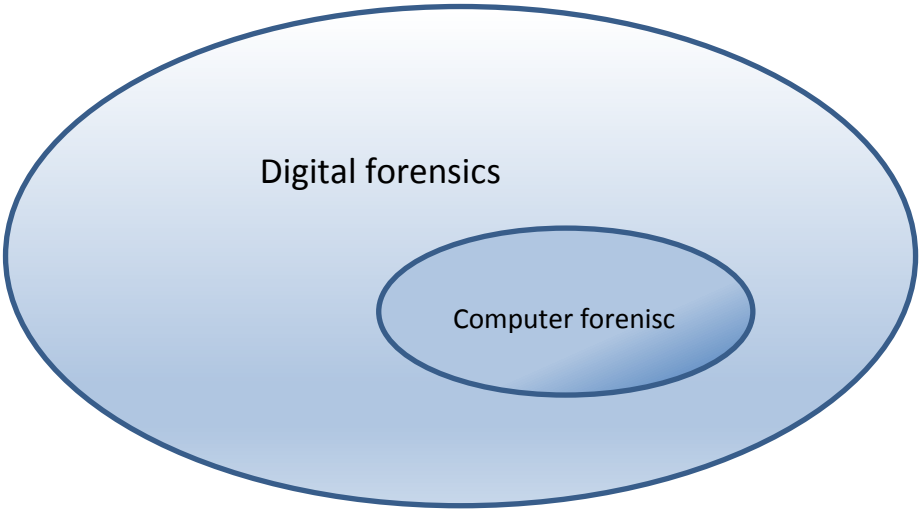


Figure 2. Digital and Computer forensic realm

Digital transformation impact on digital forensics

Digital transformation has an impact on digital forensics because of an increased number of users and digital devices.

These devices are used and sometimes misused in a way that they become objects of criminal investigations. Law enforcement agencies use sources such as personal or business computers and Internet cache history to analyse behaviour of suspects and law offenders with a goal to resolve criminal cases.

Audit vs. Digital forensic investigation

Having digital devices as means of support for business and everyday life activities poses a risk of using those devices for unlawful or other wrongdoings. To support every activity where digital data exists, there is a need to analyse and investigate how data and digital devices are being used. Two general approaches for analysing and investigating digital evidence and operation with digital data are known as audit and digital forensic investigation.

Audit and forensic investigation are not the same and based on Marcella and Mendey's (2008) comparison, this book presents some major differences between the two investigation processes.

TABLE 1. Audit vs. Digital forensic investigation

Elements	Audit	Cyber Forensic Investigation
Definition	*"Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes." (IIA, 2019)*	*"The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal…"(*DFRWS, 2001)

Objective	To determine alignment of organisational operation with law regulations, bylaws, and standards.	To detect digital evidence and identify individuals responsible for the wrongdoing.
Scope	The scope should be determined during the planning phase and it depends on the audit goals.	All digital devices which can be used to document a specific case.
Timing	Planned regular audits or audit by the request of management.	Part of the investigation process after an incident in which digital device was used.
Methodology	Professional Practice of Internal Auditing by The Institute of Internal Auditors.	Available and approved local or international methodology which defines digital forensic steps such as justification for starting the forensic investigation, getting approval for investigation, and steps for conducting forensic investigation on the scene: "*…preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources…*" (DFRWS, 2001)
Reporting	Reporting to the organisation or company management.	Reporting to prosecutor, law enforcement, or the organisational management.
Impact	Presented in a non-confronted manner, the aim is to help auditee recognise risks and improve performances and level of alignment with law and standards.	It depends on the investigation outcome.

Digital forensic process

Digital forensic process refers to the identification, preservation, collection, analysis, and reporting of evidence found on any digital device to support investigations and legal actions.

Digital forensic scope

Scope of digital forensics is not limited to specific technology, hardware, or software component, because digital evidence can be stored in a

database or file, and transferred via different network technologies. Criteria for determining scope of digital forensic investigation can be based on the object of attack or fraud, devices used for fraud or attack, and vector of the attack.

Some of these sub-disciplines of digital forensics which determine digital forensics are presented below (Open University, 2018).

Personal computers and servers

Computer forensic process is performed on computers, laptops, and storage media.

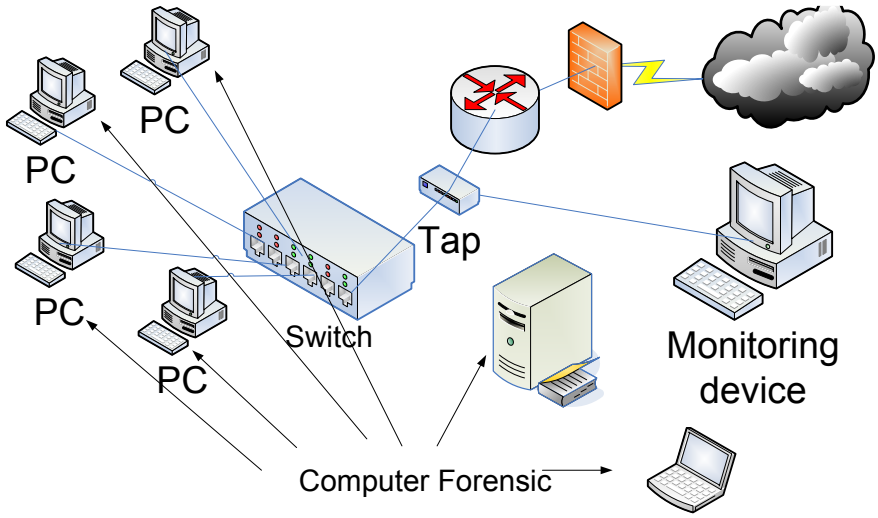


Figure 3. Computer forensic

Forensic investigators search for digital evidence in directories, files, and logs that can be stored on hard drives, and other media such as removable media used with computer systems.

Network devices and active components

Network forensic process includes monitoring and/or capturing, preserving and analysing network traffic, sessions, and other network activities or events in order to discover the source of security attacks, intrusions, or other problem incidents, i.e. worms, virus, or malware attacks, abnormal network traffic, and security breaches.

Special care must be taken in collecting forensic data in networks because network traffic has to be captured in order to be analysed. In most cases if the traffic and session are not captured, it is only possible to analyse result of sessions and traffic generated in time before the investigation took place.

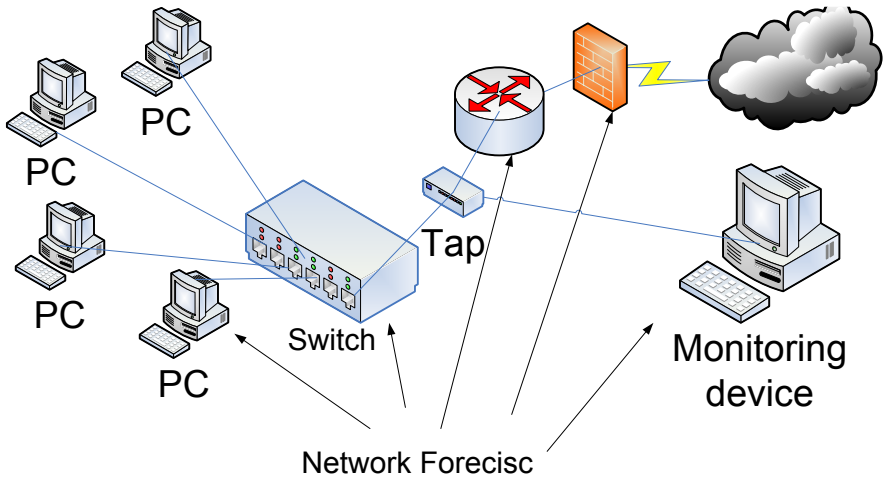


Figure 4. Network forensics

Databases

The recovery of information from databases entails the recovery of logs associated with database operations, as well as user and administrator interactions with data stored in database files and logs.

Mobile Devices

Mobile device forensics is the process of collecting and analysing electronic evidence from mobile phones, smartphones, SIM cards, PDAs, GPS devices, tablets, and game consoles.

Digital Images

Digital image forensics is the process of the extraction and analysis of digitally acquired photographic images to validate their authenticity by recovering the metadata of the image file to ascertain its history.

Multimedia

Multimedia forensics encompasses Digital Video/Image/Audio Forensics which refers to the collection, analysis, and evaluation of sound, image, and video recordings. The science in this sense refers to the establishment of authenticity as to whether a recording is original and whether it has been tampered with, either maliciously or accidentally.

Memory

Live acquisition or memory forensic process refers to the recovery of evidence from the RAM of a running computer.

Triggers for digital forensics

Different events trigger digital forensic investigation such as:

- Denial of service attacks
- Child pornography
- Domestic violence
- Using organisation's computer or other equipment for the personal benefit
- Computer fraud

- Hacking
- Blackmail
- Extortion
- Homicide cases
- Missing person
- Other cases

Events stated above trigger incident response which has to involve digital forensic process.

Forensic investigation initiation

Common practice for the forensic analysis is that law enforcement initiates the forensic analysis in a written form.

Figure 4. Forensic analysis goals to detect – who, what, when, where

Other possibilities for the initiation of the digital forensics could be company's or organisation's management with a goal of performing the

forensic analysis to determine who, what, when, and where is something done with the use of digital equipment (digital assets).

Incident response

Computer and digital forensics has to be a part of the incident response due to the fact that after each incident, proper actions need to be taken so that the future incidents are prevented, and perpetrators are punished.

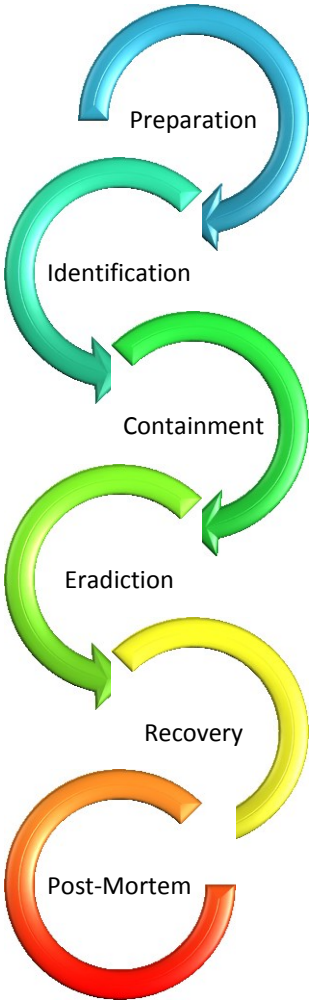


Figure 5. Incident response plan (Banking and Insurance, 2017)

Incident response is performed through predefined stages and it is usually a planned activity (Banking and Insurance, 2017). It contains stages as it is shown in Figure 5: Preparation, Identification, Containment, Eradication, Recovery, Post-Mortem. Some useful information about the recovery phase and post mortem-analysis can be found in the Appendix – Incident response form.

Post-mortem is considered to be the initial step of the digital forensic process which is explained in Chapter 3.

Summary

Digital forensics is a science about investigation where digital equipment is used to acquire relevant data for criminal investigations.

On the market, we encounter new devices, software, and services which could be the object or tool for committing a cyber-crime, which in order to be solved requires a specific knowledge to conduct a criminal investigation.

Knowledge acquired

The difference between different digital forensic types. History of forensics and digital forensics.

Review questions

1. Explain the difference between computer and digital forensics.
2. Define digital forensics.
3. What are the types of digital forensics?
4. What is the incident response and what triggers it?

5. Why is digital and computer forensics important?
6. What is digital evidence?
7. What are the basic steps of digital forensics?

Further readings

- US CERT Cyber forensic,
  https://www.us-cert.gov/sites/default/files/publications/forensic.pdf
- A Beginners Guide to Computer Forensic
  http://ithare.com/a-beginners-guide-to-computer-forensic/

Video resources

- How the Feds Caught Russian Mega-Carder Roman Seleznev
  https://www.youtube.com/watch?v=6Chp12sEnWk&t=2529s
- Cyber forensic
  https://www.youtube.com/watch?v=2D5wTo1adbg
- What is cyber forensic
  https://www.youtube.com/watch?v=lxUN-fOIe00
- What is cyber forensic, Smithsonian Channel
  https://www.youtube.com/watch?v=BSyi6yMIB0s

2. Digital forensics – classification

Chapter abstract

Chapter goals: To present different computer and digital forensic types based on data source used for the digital forensic investigation. To explain each recognised class of forensic investigation.

Learning outcomes: Knowledge of the core forensic classification and data such as database log files important for conducting the forensic investigation.

Digital forensic classification based on data source

Based on data source and scope of digital forensic explained in the previous chapter, digital forensics can be classified as following: general computer system forensics, database forensics, forensics of multimedia devices, forensics of general computer systems, mobile device forensics, and network forensics.

Figure 6. Digital and Cyber forensic types

Forensics of general computer systems

Computer systems are built on components such as motherboards, memory, hard drives, monitors, and DVD. Depending on usage and mobility, systems can be on laptop, home computer, work computer, and server in the enterprise environment. These systems can have an abundance of interesting digitally stored information needed for a potential forensic analysis. Investigators can obtain written documents with dates of creation, e-mail correspondence, pictures, messages, etc. This information can be used to determine the timeline of events and involved actors. (Casey, 2011).

Database forensics

Database forensics relies on data stored in databases and files used by database management system (DBMS).

Paul M. Wright (2007) defined major sources of evidence in Oracle database which can be considered when performing database forensics:

Listener log – This log stores the name of the listener, protocol, and communication port used for accepting connections, nodes allowed to connect to database, database services, and control parameters.

Alert log – This log stores starting and halting database, errors connected to data storage, etc.

Sqlnet log – The purpose of this log is to keep track of an unsuccessful access to a database. Forensic analyst has to check this log to discover potential unauthorised attempts to access database. This log can provide useful information about the source address of the connection establishment attempt.

Redo logs – This log holds history of all changes in a database. Every redo log file has a redo record that represents the change made in a specific block in database (Oracle, pp. 79) if Oracle archiving is activated (Litchfield, 2007). Every change in a database is written on database buffers in the system global area (SGA) memory. Buffers are stored either by issuing COMMIT command, or they are stored every three seconds on a disk in the file known as Online Redo Log by Oracle Log Writer

background process (LGWR). There is a possibility that these logs can be filed up and log files rewritten with new entries. To be able to recover important logs from database and avoid deletion of important logs it is necessary to activate Archive (ARCn) option in a database (Litchfield, 2007).

It is possible to check if archiving is turned on by issuing SQL query:

```
SQL> SELECT VALUE FROM V$PARAMETER WHERE NAME =
'log_archive_start';
VALUE
--------
TRUE
```

Value TRUE indicates that log archiving is activated, while FALSE indicates that it is not enabled.

FGA (Fine Grained Auditing) audit log can be used for collecting data about changes in a database. It tracks commands INSERT, UPDATE, and DELETE, and other changes such as data movement in a database. All detected activities are recorded in audit tables (Oracle Fine Grained Auditing, 2019).

Nanda A. and Burleson (2003) wrote:

"The ability to check who actually handles objects, not just who has authority is provided by ***auditing****. A good auditing system provides a*

process for recording the access to the objects in a storage system, forming an ***audit trail****"*

(Oracle DBA_FGA_AUDIT_TRAIL, 2019):

"Audit trail records created by Fine Grained Auditing can be captured and analysed in Oracle Audit Vault and Database Firewall, automatically alerting the security team about possible malicious activity."

Audit tables contain information presented below (Oracle Fine Grained Auditing, 2019):

DB_USER – database user which issued queries in database.

SESSION_ID – unique ID session.

TRANSACTION_ID – Transaction ID with which object is changed or accessed.

OS_USER – Operating system user.

USERHOST – name of the computer (host).

OBJECT_SCHEMA & OBJECT_NAME – scheme and table.

SCN – (System Control Number of the database) – defines when an audit trail was generated.

SQL_TEXT – text SQL commands.

COMMENT$TEXT – additional comments linked to audit if they exist.

EXT_NAME – If users are accessing from the outside, their name is displayed here.

TIMESTAMP – date and time of the audit.

The following are DBA_AUDIT tables that can be used for the forensic analysis, and which can be listed by issuing SQL query:

```
SELECT view_name
FROM dba_views
WHERE view_name LIKE 'DBA%AUDIT%' OR view_name LIKE
'USER%AUDIT%'
ORDER by view_name
```

```
DBA_AUDIT_EXISTS
DBA_REPAUDIT_ATTRIBUTE
DBA_REPAUDIT_COLUMN
DBA_AUDIT_OBJECT
DBA_AUDIT_SESSION
DBA_STMT_AUDIT_OPTS
DBA_AUDIT_STATEME
DBA_AUDIT_POLICIES
DBA_AUDIT_TRAIL
DBA_AUDIT_POLICY_COLUMNS
DBA_COMMON_AUDIT_TRAIL
DBA_FGA_AUDIT_TRAIL
DBA_OBJ_AUDIT_OPTS DBA_PRIV_AUDIT_OPTS
USER_AUDIT_SESSION
USER_AUDIT_OBJECT
USER_AUDIT_STATEMENT
USER_AUDIT_TRAIL
USER_AUDIT_POLICIES
USER_AUDIT_POLICY_COLUMNS
USER_OBJ_AUDIT_OPTS
USER_REPAUDIT_ATTRIBUTE
USER_REPAUDIT_COLUMN
```

Tables above contain data that indicate which, what, where, and when specific user made changes. This information can be used for the forensic analysis of Oracle database.

Forensic tools presented in Chapter *4. Digital forensics tools* are used for database forensic investigation to find specific evidence in a large volume of data through different files and tables in a database.

Forensics of multimedia

Multimedia such as audio, video, and pictures are sources of digital data which can be used for the forensic analysis.

Most popular devices that hold multimedia content are smart phones, however, other devices such as gaming consoles, TVs, PDAs, CCTV, other video or audio recording, and even IoT devices are also multimedia devices which can be used for the forensic analysis.

Watermarking

Watermarking of image is a process of identification of user who created it as well as the original source of that image.

Digital signatures

Digital signatures are signatures which can be found in an electronic form, and which indicate a specific originator of electronic data.

Mobile device forensics

Increased usage of mobile devices opens digital forensic area of mobile devices.

Computer systems are not only in a form of desktops, laptops, or servers. They are also produced in a form of small computers embedded into smart cards, mobile devices, GPS devices, and car computers. Mobile communication devices can contain personal information, messages, photos, and locations. Navigations systems can reveal location information of a person under the investigation. All those devices are valuable sources of information, especially because embedded devices are

usually small, and used on a daily basis and in the mobile environment (Casey, 2011).

Network forensics

Modern life is embedded into communication systems by all means. Humans, computers, and sensors all communicate through communication networks. Pieces of information are always left in the system logs, no matter what type of communication is used. Traditional telephone systems and internet service providers can be valuable points for the investigation of the digital evidence. Mobile service providers transfer SMS/MMS messages and mobile internet interconnections, while Internet service providers transfer e-mails. In addition to the exact content of the communication channel, an additional log examination can give more information about who, when, and to whom information is sent (Casey, 2011).

Network forensics is performed in order to investigate network flows, network traffic and network connections. To be able to collect and analyse network traffic, traffic has to be recorded and archived for the later use. In most organisations, this approach is not applied because it adds an additional load on the already busy network administrators. Many network devices such as switches, routers, and firewall have basic syslog capabilities which provide network administrators with information about established connections, and device operations. Syslog functionality cannot provide information about data payload inside network packets.

Summary

Cyber security is a subset of information security that deals with the security of information stored in a digital form and transferred over communication links. A great part of information security related standards deals with cyber security issues.

Almost on a daily basis, media reports reveal cyber security related incidents. After the historical analysis, we can conclude that we will see an increase in incidents of this type, especially as more services and users use digital technology in everyday work and life.

Knowledge acquired

The difference between digital forensics classification types that includes Forensics of general computer systems, Database forensics, Forensics of multimedia, Watermarking, Digital signatures, Mobile device forensics, Network forensics.

Review questions

1. What is watermarking?
2. Name digital and cyber forensic types.
3. What is network forensics?
4. What is mobile device forensics?

Further readings

- Network forensics
  https://www.itpro.co.uk/cyber-attacks/31660/what-is-network-forensic

Video resources

- Advanced Wireshark Network Forensics – Part 1/3
  https://www.youtube.com/watch?v=e_dsGhvq9CU
- Network Forensic Data Theft Detection, Under the Hood
  https://www.youtube.com/watch?v=CYRYmKhz3QI
- Mobile Device Forensics
  https://www.nist.gov/sites/default/files/documents/2017/05/08/aafs-mobiledeviceforensic.pdf
- Forensics, SANS
  https://www.sans.org/reading-room/whitepapers/forensic/paper/32888

3. Digital forensics – process

Chapter abstract

Chapter goals: To define digital forensic process which includes Preservation, Handling evidence at crime scene, Collection, Transport, Examination, and Analysis of digital evidence. This chapter briefly explains media analysis, file system analysis, network analysis, application analysis, OS analysis, executables analysis, image analysis video analysis, memory analysis, and reporting. It also provides the explanation regarding digital evidence collection and data concealment.

Learning outcomes: Knowledge of core principles of digital forensics, and different types of analysis.

Steps in the Digital Forensic Investigation Process

In order to successfully show evidence and defend legitimacy of the entire forensic process, it is necessary to perform every step of forensic investigation with sound science methods. Courts will not accept evidence if forensic process was jeopardised with negligence in evidence handling,

preservation, and transportation. Forensic investigators and examiners must be well trained and certified for forensic investigations. All actions in the forensic investigation process have to be well documented through policies and procedures. Every digital forensic investigator or agency has to follow digital forensic steps, so that reports are admissible at the courts of law.

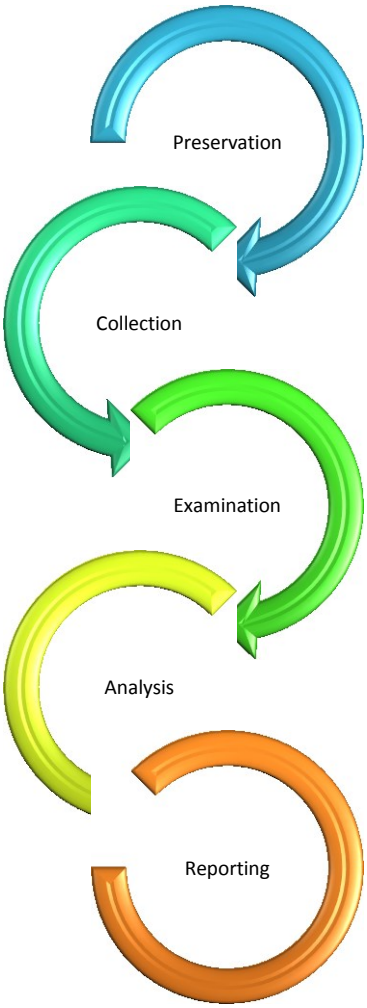


Figure 7. Steps in the Digital Forensic Investigation Process

One of the main approaches in forensic investigation is to follow well-defined and accepted digital forensic investigation steps (Kaur and Kaur, 2012):

- Preservation
- Collection
- Examination
- Analysis
- Reporting.

In Appendix – Digital forensic process are presented steps for forensic process.

Preservation

In the preservation phase, all evidence has to be properly documented to avoid any prior change of the crime scene. Crime scene has to be secured so that nothing is changed when investigators enter the scene.

Digital forensic investigators are focused on finding and preserving digital evidence, however, it is also possible that other forensic skills are needed to collect biological samples such as fingerprints, DNA, etc. All mentioned evidence has to be detected, documented, and preserved in the original form, if possible, to avoid jeopardizing data and evidence integrity. Depending on available information it is possible that digital devices are contaminated with hazardous material. In that case other forensic investigation specialists might be needed.

If a device such as PC or a mobile device is found switched off, and somebody turns it on as a part of digital forensic process, they may cause a change of potential evidence on that device, in which case evidence would lose its integrity and it would not be valid (Kaur and Kaur, 2012). Massachusetts Digital Evidence Consortium (2015) explained in their publication that first responders have to perform evidence preservation and collection with a special care. Crime scene has to be investigated with forensic methods only if law enforcement agencies approve such process.

All digital evidence such as hard disks has to be secured from the high temperature, high electromagnetic fields, and moisture. This is because such external influence can destroy potential evidence.

Forensic investigators are responsible for documenting the crime scene by taking photographs and making video recordings of the scene. It is useful to sketch the scene and keep records about investigators who were on the scene as well as their responsibilities. It is also suggested to ask owners of devices if they are willing to cooperate, and if they give their consent investigators can request passwords, PIN, or other security features. Device owner has to sign consent form with authentication methods and passwords. Owner has to provide information of other possible authentication methods such as face, fingerprint, or other biometric recognition methods used for the authentication.

At the end of this book the *Appendix – Consent form* is an example of the consent form created based on Massachusetts Digital Evidence

Consortium (2015) documentation. If the consent is not given, suspects in many jurisdictions will be fined.

The chain of custody has to be kept through the entire process. Digital evidence must be secured at all times, so that all activities performed during seizure, access, storage, and transfer can be completely documented, preserved, and authorized. Documentation which proves all of the above has to be available for the review. It needs to be emphasized that individuals are fully responsible for digital evidence while evidence is in their custody.

It is important to determine if devices are switched on or off.

If a device is switched on and then switched off, data about active connections or data from volatile memory would be lost. This is a way in which forensic investigators have to check if the device produces vibrations due to HDD operation, other sounds, and lights. Device has to be accessed with caution, by isolating it from networks such as wired, wireless, and GSM. If possible, device has to stay powered to collect all available passwords.

If a device is turned off and then switched on, potential evidence would be lost. Thus, the device has to be packed and prepared for the transportation.

Collection

Collection is the process of detecting and collecting evidence relevant for the forensic investigation. Because most of data is stored on media such

as hard disk, memory cards, and other removable media, it has to be duplicated: cloned and/or copied to media that will be used in the forensic investigation process. Forensic investigators should not change collected evidence, because in that way the investigation process would be compromised. Sources such as seized hard disc have to be secured and kept in custody while investigation is performed with cloned data (Kaur and Kaur, 2012).

Transport

There is a risk associated with a transport of digital evidence because its confidentiality, integrity, and availability can be jeopardized. Therefore, it is important that digital forensic investigators be well educated and aware of the risk associated with digital evidence transportation. Digital evidence has to be delivered to forensic laboratory in the shortest time period, and protected from external influences depending on inherited weakness of specific digital device or asset (Law Enforcement Cyber Center, 2017).

Examination

Process that defines which methods and tools have to be used in the digital forensic process is called the examination. Different devices which hold digital evidence may require different tools and methods for acquiring forensic evidence. All activities in the examination process have to be performed on cloned and copied data (Kaur and Kaur, 2012).

Analysis

Analysis refers to the process of using examined data and placing findings from the examination stage in the context for the digital forensic report. In the analysis process, available data is used to determine meaning of that data, i.e. how it was created or transferred to or from a device, and what story data tells forensic investigators. In the analysis process, forensic investigator has to acquire information about data ownership, potential hidden data, file, or application.

Types of Digital Evidence Analysis

Due to a different source and scope of data usage, digital forensic investigators are able to conduct different types of digital forensic investigation (Carrier and Spafford, 2004).

Examples of digital forensic analysis reported by Carrier and Spafford (2004) are the following:

- *"Media analysis*
- *Media management analysis*
- *File system analysis*
- *Network analysis*
- *Application analysis*
    - *OS analysis*
    - *Executable analysis*
    - *Image analysis*
    - *Video analysis*
- *Memory analysis"*

These types of analysis can be applied to computer as well as mobile devices.

Media analysis

Media analysis refers to the analysis of storage media. It does not consider any partitions or other operating system-specific structures. Storage media can be USB drive or disk, and SD cards for cameras or mobile devices (Carrier and Spafford, 2004).

Media management analysis

Media management analysis focuses on media logical organization, such as combining more disks into one logical volume. An example of combining more disks into a logical volume is mirroring of two physical disks into one logical disk. Mirroring disks in such manner means that one chunk of information is written on both disks at the same time. In case of one disk failure, another one continues to operate (Carrier and Spafford, 2004).

File system analysis

File system analysis is the analysis of the system data inside the disk or deleted files in order to extract the contents of the file (Carrier and Spafford, 2004). File system takes care of the files written across the available partition. In case a file is deleted, it is usually marked deleted, signalling to other processes that location is free to record the next data. When deleted files need to be recovered, special tools can be used to locate file fragments and rebuild them to a useful file.

Network analysis

Network analysis refers to the analysis of the data inside protocol layers (Carrier and Spafford, 2004). Network analysers can be used to reconstruct raw data packets into application layer information. Communication level is essential to reconstruct possible scenarios of user or computer interactions, and it is a very valuable source of information.

Application analysis

This type of analysis analyses data information inside the files and application. Files are created by the user, and format of the content is application-specific such as text documents or photos.

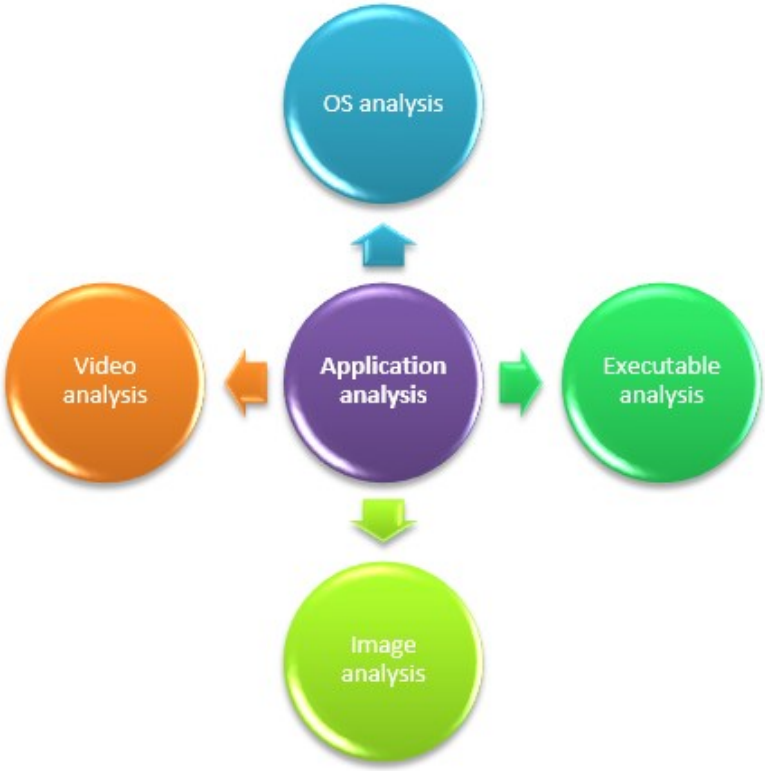


Figure 8. Application analysis

Some special types of a common application analysis are:

- OS analysis
- Executable analysis
- Image analysis
- Video analysis

Operating System (OS) analysis

OS analysis is the operating system-specific analysis of the configuration and events during usage (Carrier and Spafford, 2004). OS communicates with hardware and upper layers. All interaction details such as errors, warnings, different types of events as well as configuration, are recorded and stored inside OS compartments. This information can help build the overall digital landscape.

Executable analysis

Executable files can cause events and they are noticed when executed as processes. Executables such as malwares are common for the analysis during the intrusion investigation (Carrier and Spafford, 2004).

Image analysis

Image analysis refers to the analysis of the person recorded on image, location, or timestamp. Image analysis includes the analysis of the potential steganography information (Carrier and Spafford, 2004).

Video analysis

Video files are the subject of the analysis of surveillance cameras, web camera, and smart phone camera. Same as image analysis, video analysis

leads to information about person, location, or timestamp (Carrier and Spafford, 2004).

Memory Analysis

Memory analysis can reveal very useful information, because it is used for dynamic operations and storage of temporary results.

Operating systems use two types of memory:

a) The volatile memory (RAM) is a fast memory used for dynamic operations. It stores data until device is switched off. The main function of volatile memory is to store application and system data during runtime, which contain information such as password, usernames, session data, encryption keys, data about activities and network, etc.
b) The non-volatile memory refers to the internal storage such as flash memory and equipment extensible storage device known as the SD card. This type is mainly used for static data storage such as application and system data, user settings, and data files. Data is stored even after device restarts or powers off.

Reporting

Reporting is the final word about findings. Examiner is responsible to write an accurate and complete report on findings and analysis of the digital information and device. In addition to findings and analysis, it is important to have accurately documented steps taken during all phases of the investigation.

General suggestions for the information that could be included in the report is the following (National Institute of Justice, 2004):

- Identity of the reporting agency
- Case identifier or submission number

- Case investigator
- Identity of the submitter
- Date of receipt
- Date of report
- Descriptive list of items submitted for examination, including serial number, make, and model
- Identity and signature of the examiner
- Brief description of steps taken during the examination, such as string searches, graphics/image searches, and recovering erased files
- Results/conclusions

Digital Evidence Collection

Every digital forensic investigator must be aware of the entire context of digital surroundings and other sources of evidence at the crime scene. Every digital device, if accessed in an improper manner, can cause data change and evidence loss. Data can be in form of network connections, processes, memory data, and data on hard disk or peripheral memory, or in volatile and non-volatile memory. Data written on mobile device memory cards, hard drive, and external memory storage can be considered as static memory or non-volatile, while data written in RAM is considered as volatile memory.

With this in mind, it is important to distinguish states in which data can be found. Furthermore, digital forensic investigator has to be careful in approaching data collection phase.

Computer or other digital devices which are recognised at the crime scene must be approached with care. Crime scene has to be preserved and documented using sketches and photos, and if computer or other digital devices are found, their power status must be checked.

Hard drive data will remain on media after a device is powered off and that data can be cloned and duplicated. Data in RAM will disappear after device is turned off. This includes information such as running processes, network connections, and system settings (Nelson, Phillips & Steuart, 2015). This is the way in which two major approaches have to take care of live data and post-mortem data acquisition.

Live Data collection

Tools for the acquisition of data in volatile memory can copy data from volatile memory and transfer it to the forensic location on non-volatile memory for the later analysis. Data from volatile memory or system can also be copied with the goal to collect information such as established sessions, running processes, network processes, passwords, and connected users.

Live acquisition is done if a digital forensic investigator decides to collect all available data in volatile memory from the crime scene. Digital forensic investigator needs to be aware that any access to running system can change data and destroy evidence on that system.

Data acquired from volatile or non/volatile memory has to be copied or cloned on a disk which will be used for the forensic analysis. During this

phase, all data dumps must be saved on a separate disk and calculated with hash functions such as SHA512 to be able to have a guaranteed evidence integrity. All results from hash calculation such as SHA512 have to be saved for the later use.

Data that can exist in a volatile memory is the following:

- Information about running processes, network sessions, and services
- Unpacked/decrypted versions of protected programs
- Running malware/Trojans
- Cloud service information
- System information (system uptime, system inventory, etc.)
- Information about logged in users
- Registry information
- Open network connections and content of ARP cache tables
- Social networks information
- Online communication (Viber, Skype)
- History of Web browsing activities
- Information about an access to Webmail systems
- Decryption keys for encrypted volumes mounted at the time of the capture
- Recently viewed images

Information about running process, open network connections, and evidence will not remain after the process is completed, which is due to volatile memory data limitations. However, with types of data such as web browsing history, online chats will not disappear instantly after the end of

communication. System or its user can overwrite data (Afonin and Gubanov, 2013).

Post-mortem data collection

Digital device which is powered off is ready for the post-mortem data acquisition. Only approved tools for data imaging are used for the post-mortem forensic data acquisition. For data acquisition it is necessary to make a clone and perform the forensic analysis with cloned and copied data while original media stays intact in the safe place with calculated hash value such as SHA512. Devices which prevent changes on the original device with data are called write blockers. This type of devices disables writing on the original storage media. Direct access to disk plates and memory chips is enabled if a device is damaged. Forensic computer which has tools and ports able to access external devices with cloned data is used for accessing data on the cloned disk.

Completeness and accuracy are two critical measurable attributes of the acquisition process.

While completeness quantifies whether all the data was acquired, accuracy quantifies the correctness of acquired data.

In order to achieve completeness and accuracy in copying data from the original source, bit-for-bit copy and bit-stream duplicate data from the original data source to destination memory location. Bit-for-bit can be used with specialized tools, while bit-stream can be performed with the computer (NIST, 2004).

Data concealment

It is not possible to investigate data which is not available and visible to the investigator. Thus, criminals and wrongdoers employ different techniques to destroy and hide evidence (Marcella A. J. and Menendez D., 2008).

Spoliation

Spoliation is an act of destroying or changing evidence with the goal to make evidence unusable.

Encryption

Encryption is a process of converting data and files into cryptic form so that data can be accessed only by using passwords for symmetric encryption and using private and secret keys if asymmetric encryption is used.

Steganography

Steganography is the process of hiding data such as messages into existing files which can be textual files, pictures, and video files. Various tools are being used for performing data concealment in data files.

One of the well-known tools for hiding messages in data files is snow tool (SNOW, 2019) which uses whitespace steganography practice. This program is used:

"to conceal messages in ASCII text by appending whitespace to the end of lines. Because spaces and tabs are generally not visible in text viewers, the message is effectively hidden from casual observers. And if the built-

in encryption is used, the message cannot be read even if it is detected." (SNOW, 2019)

For the purpose of explaining the process of hiding the text inside the file, *"sample_file.txt"* was created with the content shown in Figure 9.

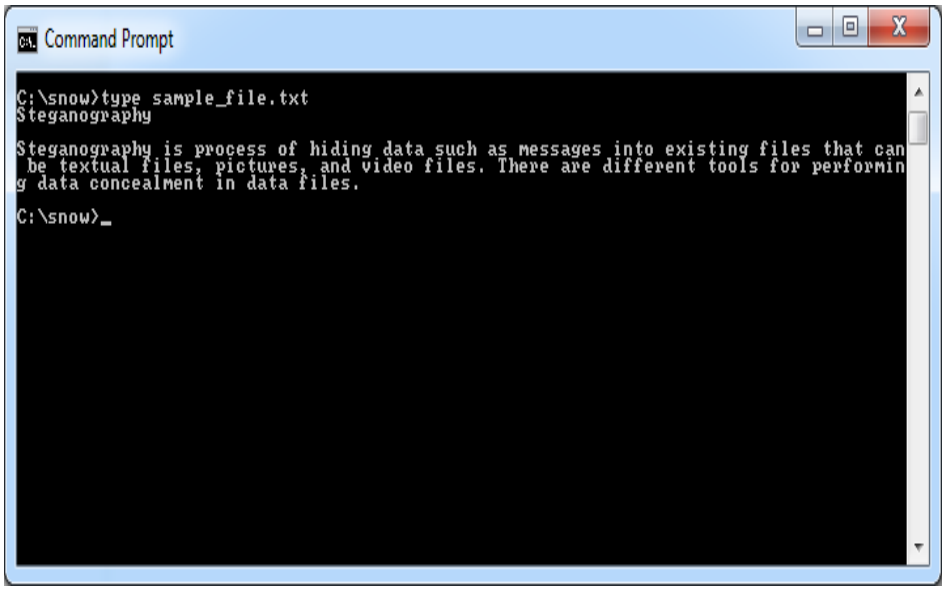


Figure 9. Sample_file.txt content

Issuing snow command with flags –C program snow compresses the data if concealing, or uncompresses it if extracting the file. *(SNOW, 2019)*

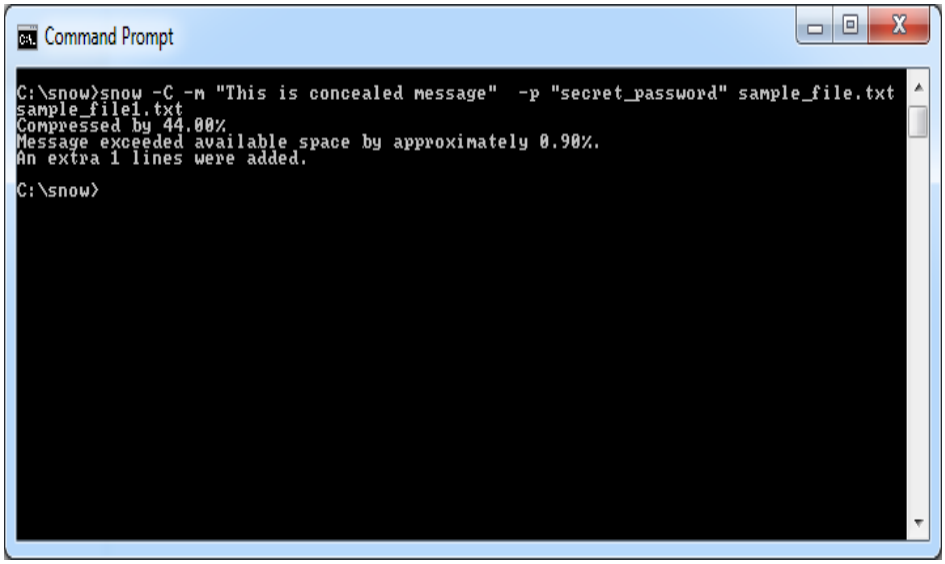


Figure 10. Creating concealed message in sample_file1.txt content

In Figure 11. it is possible to see content of the new file "*sample_file1.txt*" after issuing the type command. Figure 11. also shows in *"cmd"* editor that additional space is added but no content is visible.

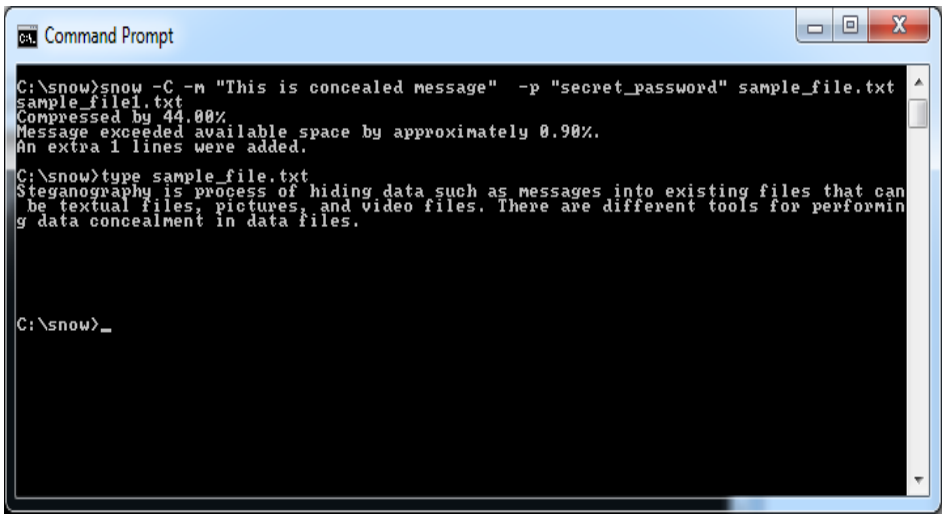


Figure 11. Creating concealed message in sample_file1.txt content

Figure 12. shows an unsuccessful attempt to read a concealed message without the password as well as a successful attempt by providing the password with *"-p"* flag that is *"secret_password."*

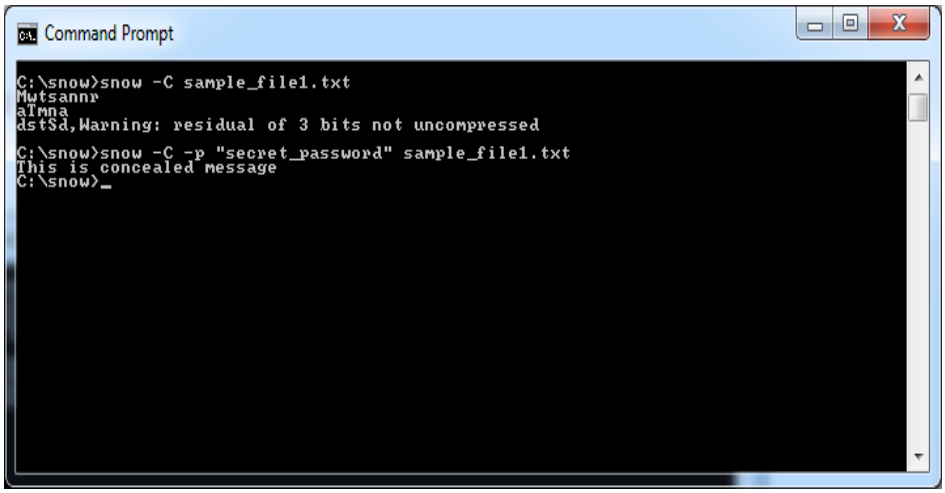


Figure 12. Reading concealed message in sample_file1.txt content

To make it harder for the investigators to find concealed data, it is possible to replace the original with the file which contains a concealed message by deleting the original file, and renaming the file with concealed message with an original file name.

Figure 13. shows the size difference between *"sample_file.txt"* and *"sample_file1.txt."* Due to such calculation of files, hash is the technique which can be used to detect if somebody, in person or by using a malicious program, changed the content of the files.

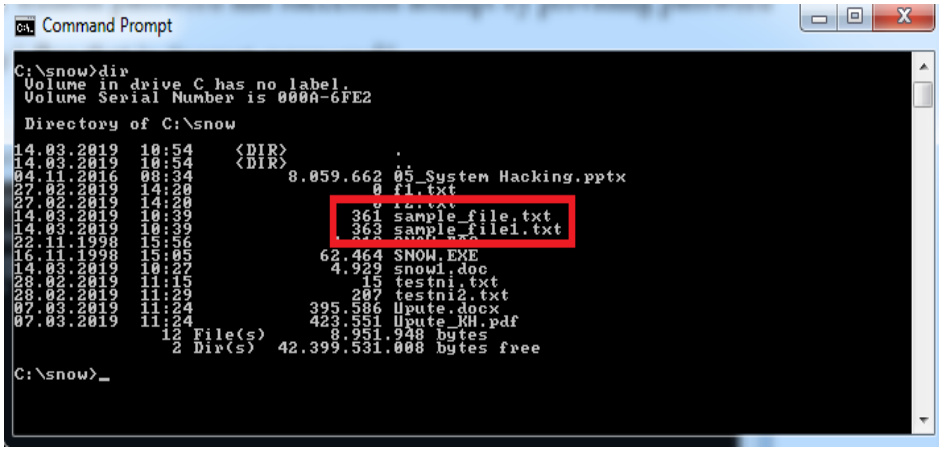


Figure 13. File sizes comparison

Summary

With a goal to successfully present forensic findings, it is necessary to conduct forensic investigation with care and by the latest forensic investigation advancements.

Every forensic investigator has to know that suspects can hide data using different techniques such steganography, encryption, or simply by destroying data.

It is important to emphasize that before the analysis, data has to be copied. The preferred action is to clone data from the original media to avoid deletion of the original data.

Knowledge acquired

Common steps in the digital forensic investigation process that includes Preservation, Collection, Transport, Examination, Analysis. Essential knowledge of types of digital evidence analysis that includes Media analysis, Media management analysis, file system analysis, network

analysis, application analysis, operating system analysis, executable analysis, image analysis, video analysis.

Memory Analysis, Reporting. Digital evidence collection that includes Live Data collection Post-mortem data collection and data concealment methods which can be used such as spoliation, encryption, and steganography.

Review questions

1. Explain common steps in the digital forensic investigation process.
2. Name digital evidence collection methods?
3. What is image analysis?
4. What is video analysis?

Further readings

- Digital transformation: online guide to digital business transformation https://www.i-scoop.eu/digital-transformation/
- The Cyber Security Management System: A Conceptual Mapping, SANS Institute InfoSec Reading Room https://www.sans.org/reading-room/whitepapers/basics/cyber-security-management-system-conceptual-mapping-591

Video resources

- Computer Forensic Investigation Process

https://www.youtube.com/watch?v=NmuhGa4QekU

- Overview of Digital Forensics

https://www.youtube.com/watch?v=ZUqzcQc_syE

4. Digital forensics – tools

Chapter abstract

Chapter goals: To present forensic tools and explain for what purpose they can be used in digital forensic process investigation. Digital forensics covers different technologies and components, hence, different and specialised digital forensic tools exist, namely for database forensics, network forensic, and mobile devices.

Learning outcomes: Knowledge of digital forensic tools and how they can be used.

Digital Forensic Tools

To achieve desired results, scope of the investigation must be defined first. Defining scope will also determine what the investigator is looking for, how to reach those locations and information and which tool has to be used. Concerning forensic tools, there are many ways to reach the same goal. This section will focus only on Android tools needed to perform the necessary steps.

Hardware digital forensic tools and their usage

Hardware tools are necessary for accessing data on devices such as hard drives or mobile devices. One of the most important aims is to clone data from original digital devices and provide the exact digital copy which will be used for the investigation.

Usage of hard disk docking stations

Hard disk docking stations should be in the arsenal of every digital forensic investigator.

This type of devices should be able to access different types of disks which can be found in laptops, personal computers, and servers. It should also have the clone function for cloning HDDs without laptop, PC, or server to prevent losing or changing files of suspects.

Figure 14. Hard disk docking station (Renkforce, 2019)

Usage of memory card docking stations

Many devices such as smart phones, laptops, and CCTV cameras hold SD memory and other types of memory cards which have to be investigated.

Figure 15. Memory card docking station (Logilink, 2019)

Memory card docking station is used to read data from memory cards taken from the device.

Usage of Portable Computer Forensic Lab

Figure 16. shows the specialised all-in-one case called Road Master (Road MASSter 2, 2019).

Figure 16. Portable Computer Forensic Lab Road MASSter 2, 2019

The Road Master is capable of high-speed forensic data acquisition operations used to access external devices.

Usage of General Computer forensic tools

Different hardware and software tools are used to preserve and collect crucial data for the forensic analysis process.

Disk Genius usage

DiskGenius is a software with functions able to recover partitions and make data backups, and it has other disk utilities required for the disk management.

It can manage storage space, deletion acts, and virus attack; it also has the formatting function, and recovers data lost due to the disk corruption, etc., and it provides the backup to prevent data loss.

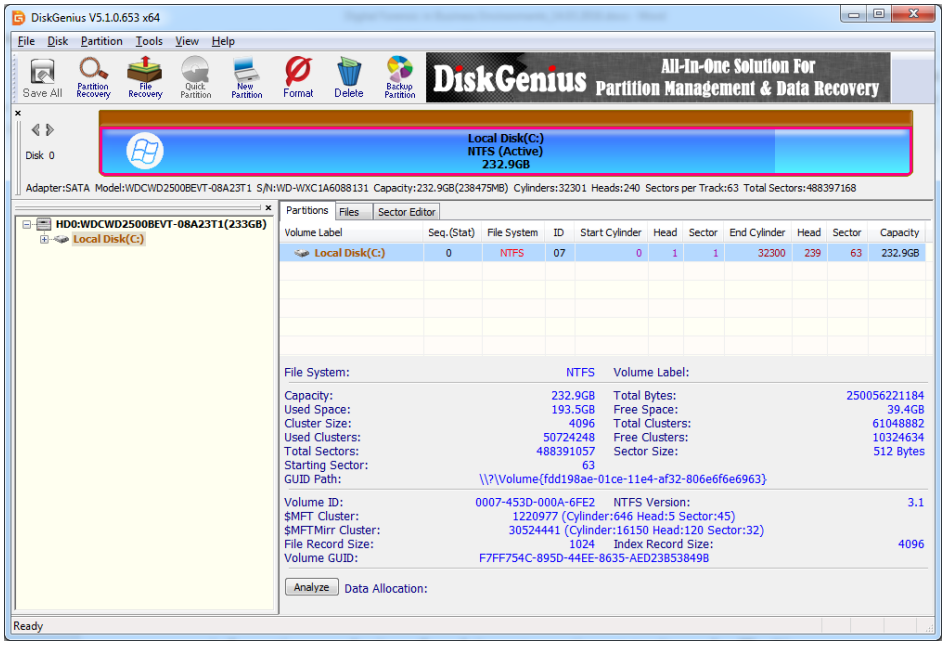


Figure 17. Disk Genius

DD command tool usage

Mobile device, computer, or any other digital device found at the crime scene can be a subject of the post-mortem data acquisition. This is a way of collecting data information on devices found switched off. Since a device if off, volatile data in memory is not available, but data stored on a hard drive/solid memory is a very valuable source of information. Investigator must make an image of a hard drive or mobile device solid memory or some other storage devices.

Linux command line dd is used to copy the content of a seized device. Example of dd usage is: dd if=/dev/sda of=/dev/sdb and it copies the content from /dev/sda to the /dev/sdb destination.

Busybox usage

Busybox is a toolset based on many UNIX utilities. Utilities are combined into a small executable. Busybox provides a usable environment for small or embedded systems. It is very modular, and it is made for limited resources. Busybox set of commands makes access to the system at a lower level making environment more accessible. It is available for download on https://busybox.net/.

Hash Calculation

Calculation of file hashes must be done immediately after the acquisition of digital information. It ensures the integrity of the collected data. It is usually a solid memory image or a separate file.

Linux commands used for generating hash values are sha256sum or sha512sum. SHA256SUM uses 32-bit blocks, while SHA512SUM uses 64-bit blocks.

Figure 18. is an example of generating hash values of usb_modeswich.conf file using both generators.

```
nera@nera-virtual-machine:/etc$ sha256sum usb_modeswitch.conf
f6c7424c7d079fa8765bf7390b400cfadfbfb89d6bd41ee7a55125e46b525e60  usb_modeswitch
.conf
nera@nera-virtual-machine:/etc$ sha512sum usb_modeswitch.conf
213afc2b713614f328b449fbf4bdc299fb596d8ee3c602508956196c14b58202a3aa7bfb5cb29867
45b20f461c6edaaeb96cf2475640e299c5e93ce9c6cae72d  usb_modeswitch.conf
nera@nera-virtual-machine:/etc$
```

Figure 18. Calculating Hash Value

Database tools usage

The following passages present tools which can be used for the database forensic process.

Usage of the Oracle LogMiner

Oracle LogMiner, (2019) is a tool that can be used for digital forensic investigations.

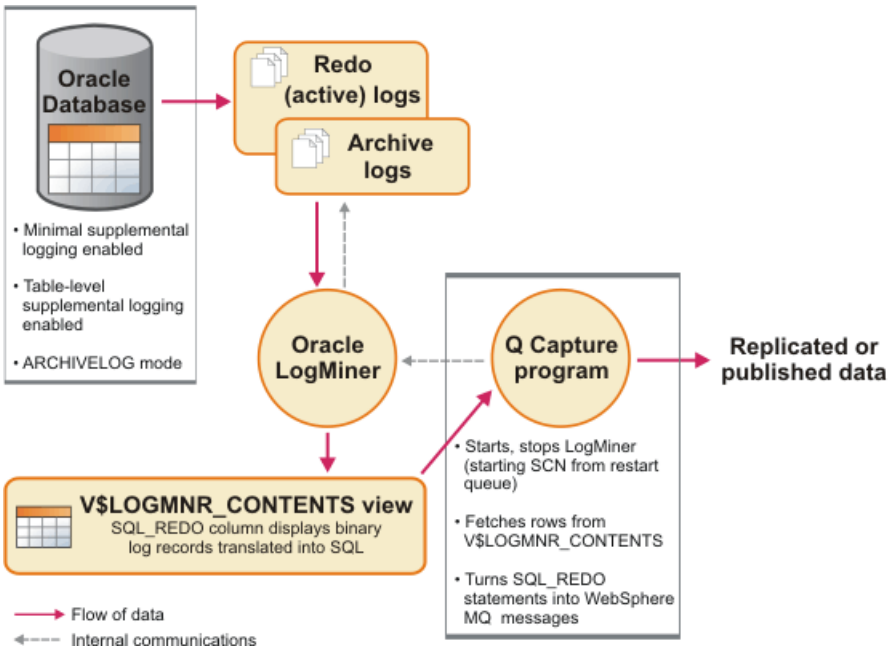


Figure 19. Q Capture program works with LogMiner to retrieve changed data IBM Knowledge, Center, 2013

It allows the analysis of changes to be performed in a database, and provides the rollback function for data including errors made by users.

Figure 20. shows how with LogMiner it is possible to view and save redo logs, as well as create and execute queries to find specific actions using GUI. It also shows query for a specific time and database user.

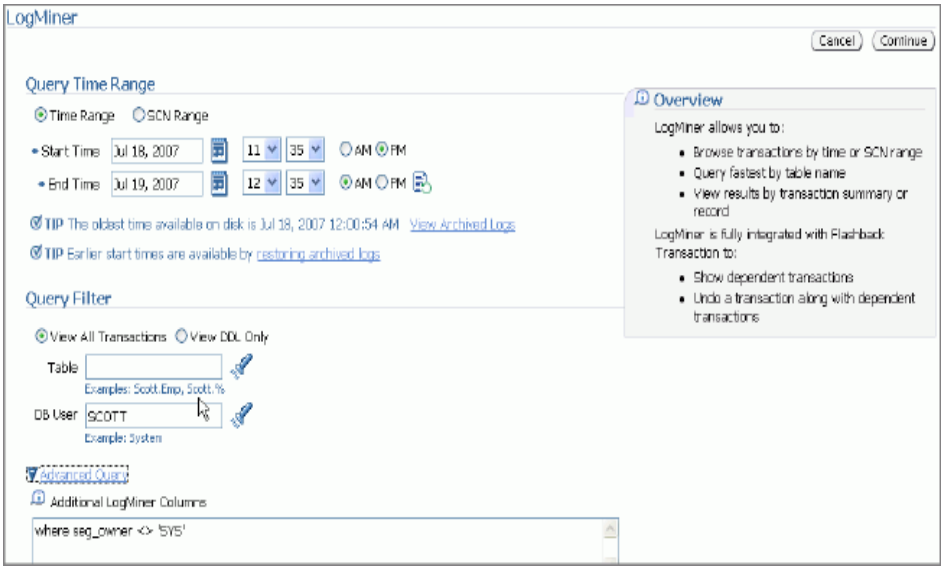


Figure 20. View all transactions for user, Nanda A., 2019

As a result, Oracle LogMiner created an initial report which shows database user activity.

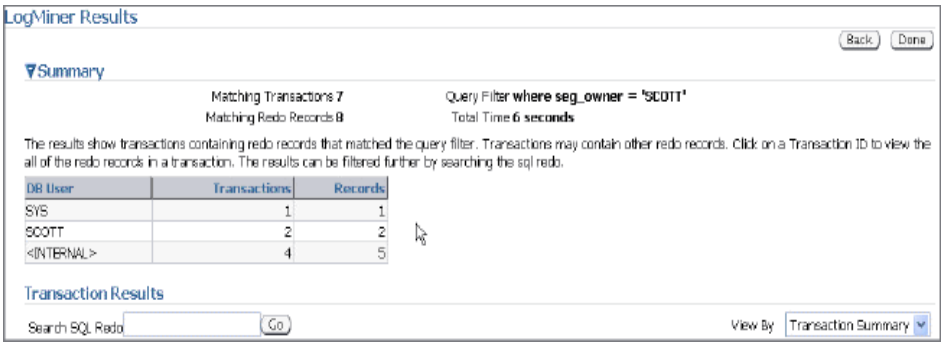


Figure 21. LogMiner results, Nanda A., 2019

By opening transactions detail, it is possible to see which query a specific user issued. LogMiner can be used for acquiring data on usage of data manipulation language (DML) which is a programming language used in a database for adding (inserting), deleting, and modifying (updating) data. The goal of using the Oracle LogMiner is to find DML statements for the post-mortem forensic investigation.

Transaction Details

Flashback Transaction | Previous Transaction | Next Transaction | OK

Transaction ID 04001F0084030000 | Start SCN 985360 | Start Time Jul 19, 2007 12:39:02 AM
DB User | Commit SCN 985362 | Commit Time Jul 19, 2007 12:39:04 AM
OS User | Machine Name

SCN	Operation	Schema	Table	SQL Redo
985362	START			set transaction read write;
985362	INSERT	SCOTT	RES	insert into "SCOTT"."RES" values "RES_ID" = 100002, "RES_DATE" = TO_DATE('19-JUL-07', 'DD-MON-RR'), "HOTEL_ID" = 12, "GUEST_ID" = 1;
985362	COMMIT			commit;

Figure 22. LogMiner results, Nanda A., 2019

LogMiner can be used for an offline analysis of archived redo logs on a separate database.

Usage of the IBM Guardium Data Protection for Databases

IBM Guardium (2019) Data Protection for Databases is a forensic tool used to protect database from an unauthorised access. It detects unusual activities on sensitive data. It provides a real-time monitoring and alerts on suspicious activities.

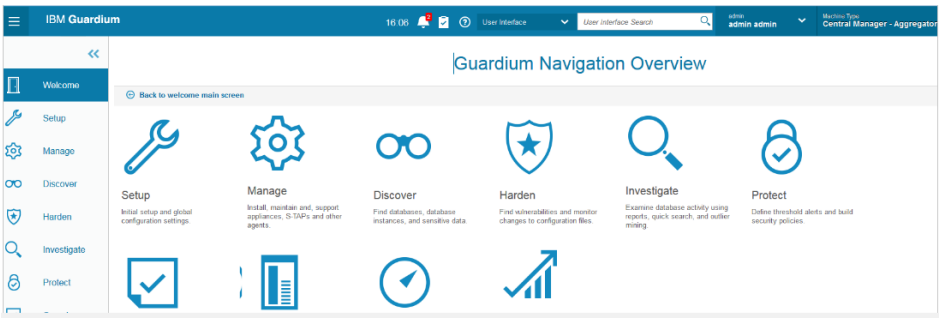


Figure 23. IBM Guardium (2019) Navigation Overview

IBM Guardium provides a preventive protection, but it can also be used for database forensic investigations which need to show if the user or administrator committed a suspicious or criminal activity.

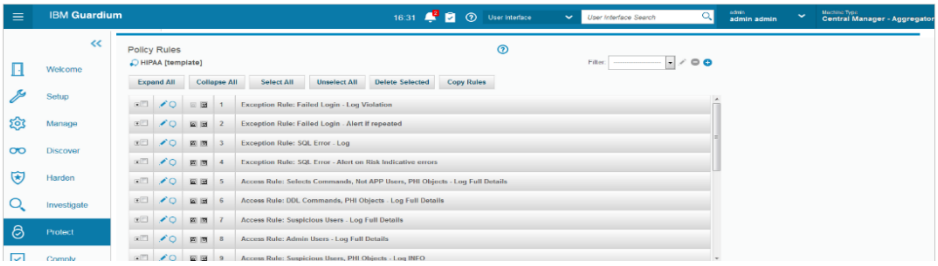


Figure 24. IBM Guardium (2019) Out of the box creation

Usage of the DB Browser for SQlite

Even small devices such as mobile phone, tablet, or embedded systems based on Android operating system utilize databases needed for services they are produced for. Regardless of whether data is structured or repeating, Android stores data in the SQLite database. SQlite is an embedded SQL database engine. Unlike other, SQL databases does not have a separate server process, which means it reads and writes directly to disk files. The entire database is contained in a single file located on a disk. Considering that size of the library is approximately 300-500 KB, and it is made to run under a minimal stack space (4KB) and heap (100KB), SQLite is ideal for devices struggling with memory space such as tablets, GPS navigations, MP3 players, etc. It is free for use regardless of being commercial or a free project.

Since each Android device consists of more databases of this type, for the forensic investigation, it is helpful to have a tool for a direct access to database. One of such free tools is DB browser for SQLite shown in Figure 25.

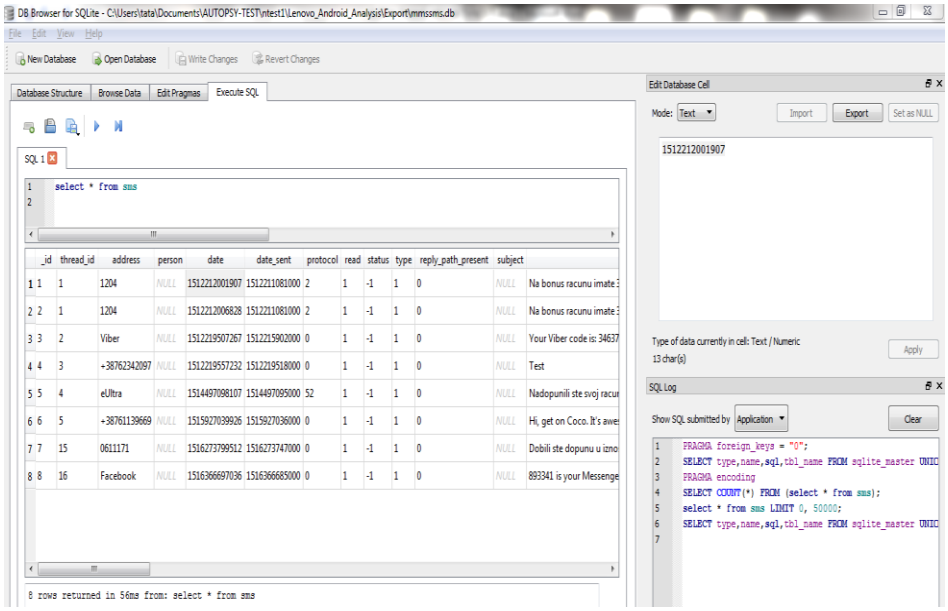


Figure 25. DB Browser for SQLite

Usage of the Undark - a SQLite data recovery tool

Undark is a data recovery tool for SQLite databases. It is useful to retrieve deleted data from the database file. Chances to recover a useful set of data are minimal if database is defragmented and vacuumed. Undark relies on the fact that actual data is not purged immediately when the process of deletion started, because there could be active transactions which could still access the old version of the record. It is rather performed at a later stage when system does periodical checks for the old data record. Download is available at GitHub https://github.com/inflex/undark.

Undark capabilities are to:

- Retrieve most available records from the SQLite database;
- Deposit actual records;
- Recover deleted records;

- Retrieve data from a corrupted SQLite database.

The command to convert the recovery SQLite database broken.db into recover.csv file format is:

```
undark -i broken.db > recover.csv
```

Recover.csv file will be filled with actual and recovered records from broken.db.

Usage of the SQLite-Deleted-Records-Parser

This is another useful tool used to recover SQLite deleted records. It is simple to use, but results are valuable in recovering deleted data from an unallocated space. Download is available on https://github.com/mdegrazia/SQLite-Deleted-Records-Parser.

Command for its usage is:

```
sqlparse_CLI -p -f source.db -r -o dbreport.txt
```

Usage of the Network forensic tools

Different network forensic tools can be used, however data and session traffic have to be captured and stored in order to have all relevant information available for forensic purposes.

Wireshark usage

Wireshark is a popular tool for capturing and analysis of the network traffic.

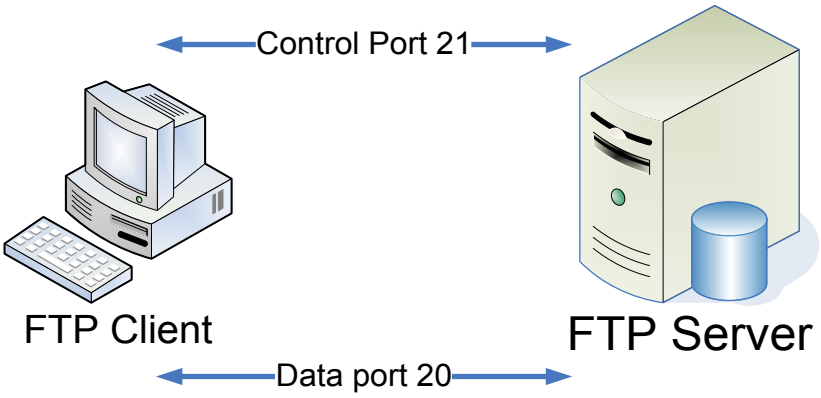


Figure 26. FTP connection

Figure 27. shows the captured Wireshark traffic for the FTP session initiation with an entered username and password as an example of how the unencrypted traffic can be captured for a later analysis.

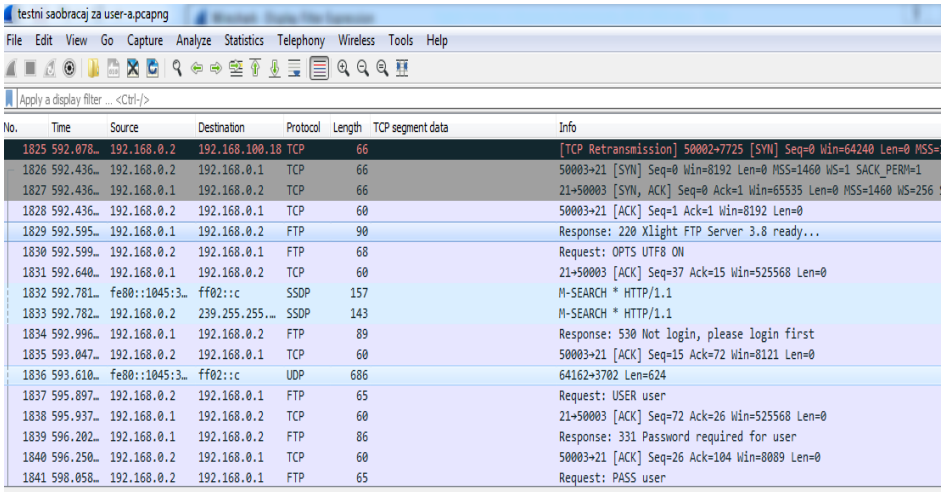


Figure 27. Captured FTP connection with Wireshark

NIKSUN NetDetector usage

NIKSUN NetDetector (2019) is capable of a dynamic application recognition, and it has integrated anomaly and signature-based IDS, data leakage prevention, real-time surveillance and application, and session reconstruction. NetDetector web site is the following: https://www.phoenixdatacom.com/product/niksun-netdetector-packet-capture-network-security-forensics/

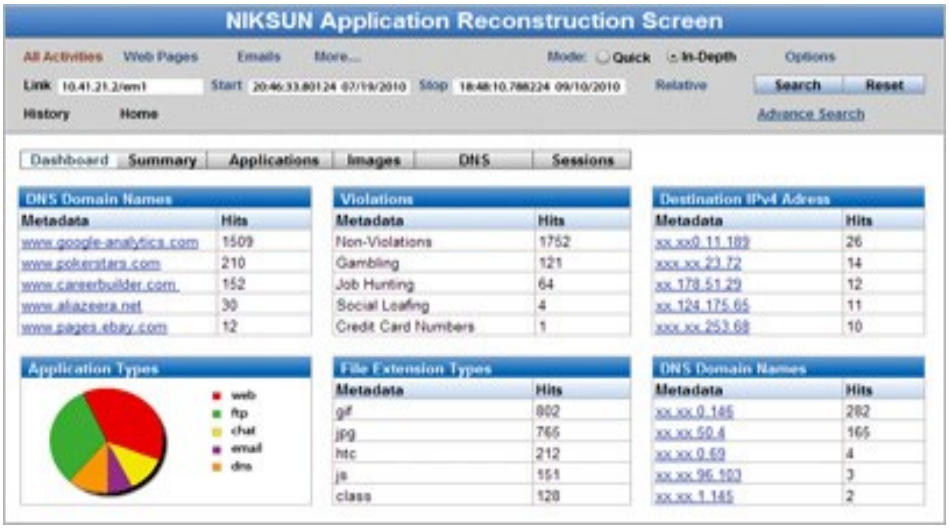


Figure 28. NIKSUN NetDetector, 2019

Xplico usage

Network forensic tool Xplico is an open source software used for the analysis of network sessions. Xplico web site is https://www.xplico.org/

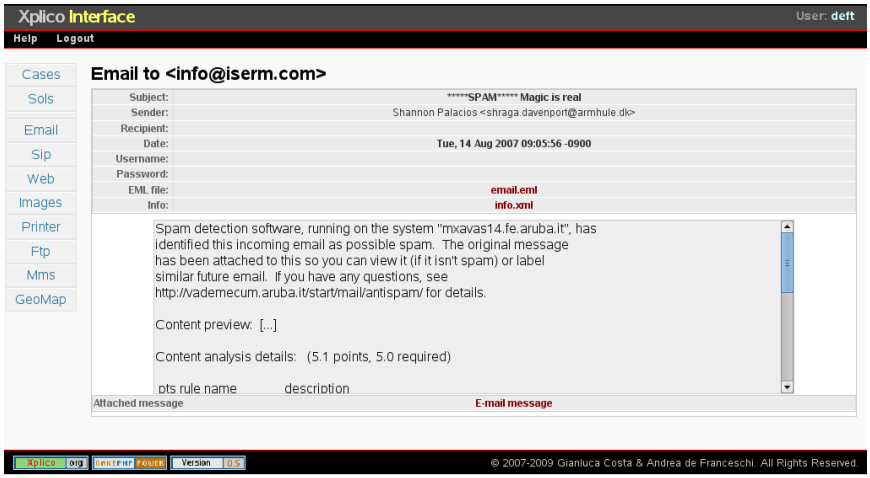


Figure 29. Xplico (2019)

Usage of the Mobile device forensic tools

General forensic tools for computer system and database tools can be used to perform the forensic analysis of mobile devices.

Rooting Tools usage

Investigator needs to decide what type of rooting needs to be performed, with or without a computer. Whatever the choice is, it should produce the same result, which is for a device to be rooted. However, a higher success rate is expected for the computer driven process. If a device needs to be rooted without the computer, a special crafted apk package needs to be downloaded and installed directly to the Android device. Very commonly used tool to root over the computer is Kingo Root (Figure 30).

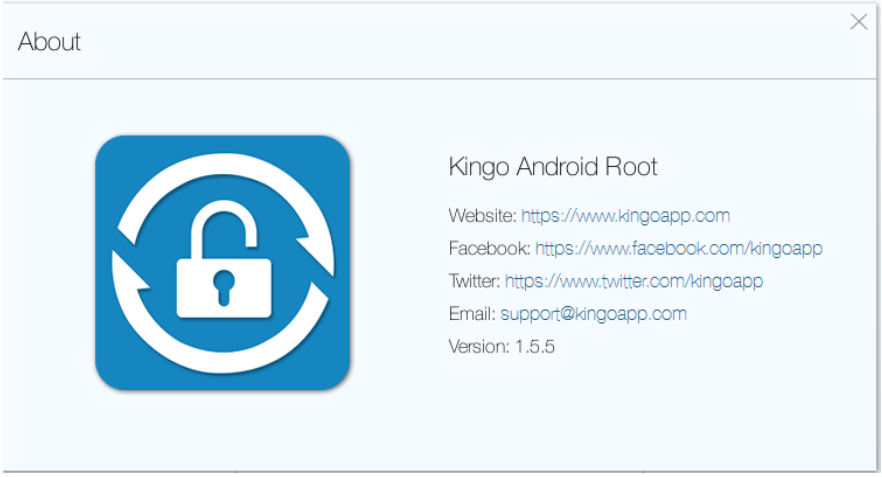


Figure 30. Kingo Android Root

If the rooting process needs to be performed without the computer, then this task can be done with an application named TowelRoot. Software can be downloaded at https://towelroot.com/

Santoku usage

Santoku is a Linux based platform used for various security related activities. Operating system comes with the pre-installed platform Software Development Kits (SDK), drivers, and utilities.

Santoku auto-detects and sets up new connected mobile devices, saving time for investigation tasks. A graphic User Interface (GUI) tool makes an easy deployment and takes control of mobile applications and investigation tools as shown in Figure 31.

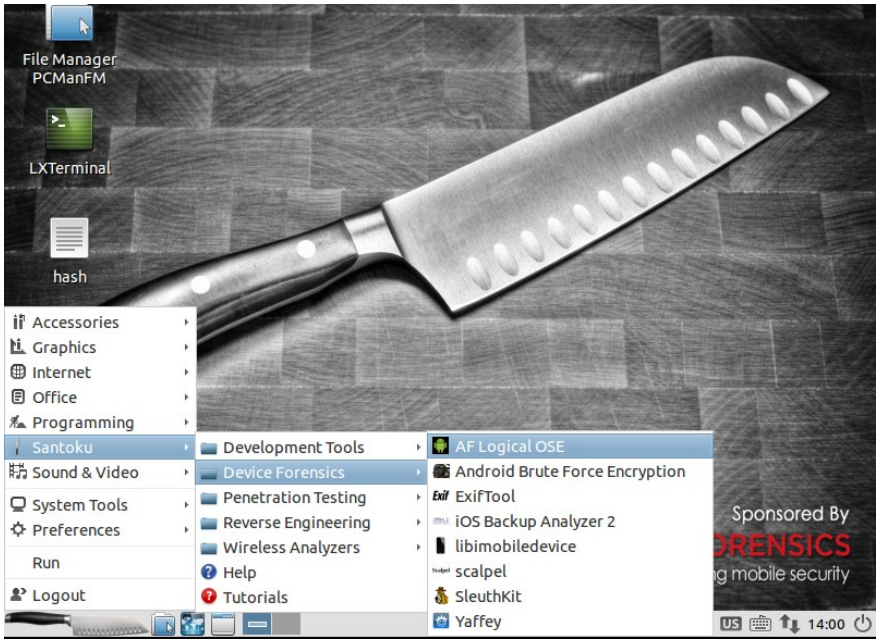


Figure 31. Santoku Linux

The installation is free for download at http://santoku-linux.com (Figure 32), and the platform can be installed on hardware or in the virtual environment.

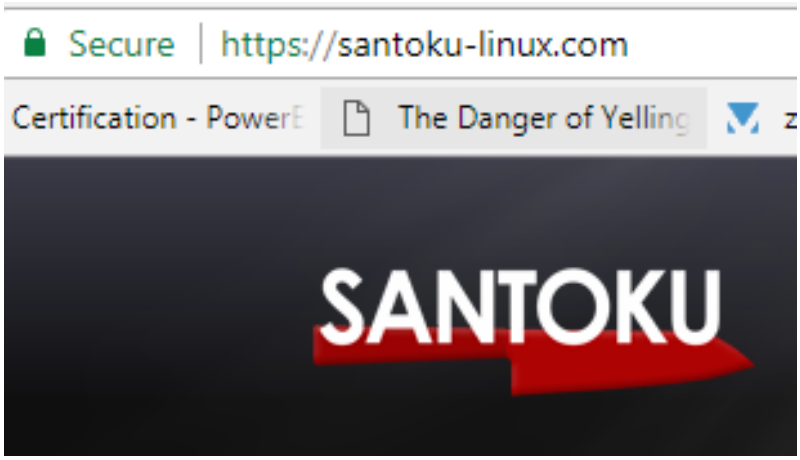


Figure 32. Santoku Linux Download

The main aim of Santoku platform is:

Mobile Forensics

Tools to acquire and analyse data

Firmware flashing tools for multiple manufacturers

- Imaging tools for NAND, media cards, and RAM
- Free versions of some commercial forensic tools
- Useful scripts and utilities specifically designed for mobile forensic

Mobile Malware

Tools for examining mobile malware

- Mobile device emulators
- Utilities to simulate network services for dynamic analysis
- Decompilation and disassembly tools
- Access to malware databases

Mobile Security

Assessment of mobile applications

- Decompilation and disassembly tools
- Scripts to detect common issues in mobile applications
- Scripts to automate decrypting binaries, deploying apps, enumerating app details, and more.

AF Logical OSE usage

AFLogical OSE is an open source tool used for a simple logical acquisition of data from the Android device. It can be found already compiled in Santoku Linux distribution (Figure 33).

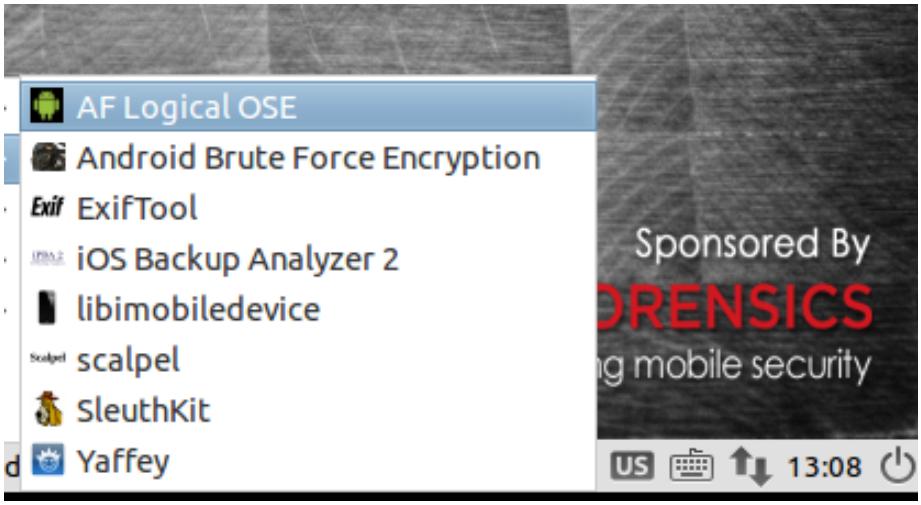


Figure 33. AFLogical OSE

Autopsy and the Sleuth Kit usage

The Sleuth Kit is an open source digital forensic set with the collection of command line tools. Autopsy is a graphical interface (Figure 34.) for the Sleuth Kit and it provides an easy usage of available tools. It also provides case management, image integrity, keyword searching, and other operations without the need for an external software.

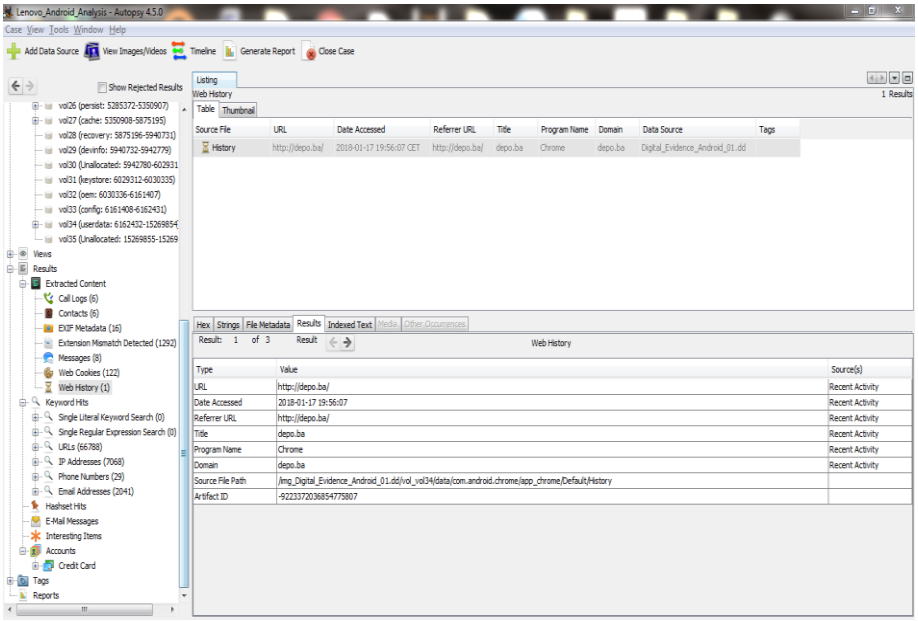


Figure 34. Autopsy Main Operations Screen

Image Import and Supported Image Formats

Autopsy can analyse raw, dd, or E01[1] format of disk images and local drives, or a folder of local files. Before the analysis, investigator is required to choose which type of data source is the source of information (Figure 35.). Forensic investigator can select Disk Image or VM File obtained with available methods, attached Local Disk, already prepared Logical Files, or Unallocated Space Image. It is possible to use a file taken out of the disk image section for an additional investigation.

[1] The popular commercial forensic suite, EnCase, developed a proprietary format called EnCase Evidence File format. EnCase Evidence Files use the file extension, E01, and are based on the Expert Witness Format (EWF) by ASR Data (Forensicwiki, 2012). These image files are commonly referred to as Expert Witness, E01 or EWF files.- (https://www.sans.org/reading-room/whitepapers/forensic/forensic-images-viewing-pleasure-35447,10.1.2018)

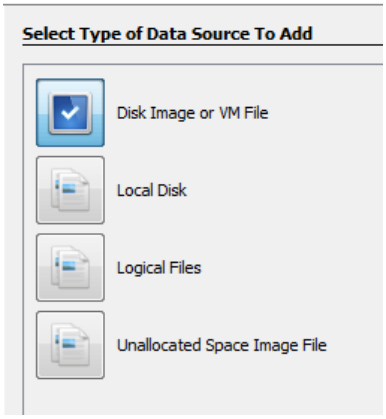


Figure 35. Type of Data Source

Analysis Features

Below is the list of Autopsy features.

- Multi-User Cases: Collaborate with fellow examiners on large cases.
- Timeline Analysis: Displays system events in a graphical interface to help identify the activity.
- Keyword Search: Text extraction and index searched modules enable you to find files which mention specific terms and find regular expression patterns.
- Web Artefacts: Extracts web activity from common browsers to help identify user activity.
- Registry Analysis: Uses RegRipper to identify recently accessed documents and USB devices.
- LNK File Analysis: Identifies shortcuts and accessed documents.
- Email Analysis: Parses MBOX format messages, such as Thunderbird.

- EXIF: Extracts geo location and camera information from JPEG files.
- File Type Sorting: Group files by their type to find all images or documents.
- Media Playback: View videos and images in the application and there is no need for an external viewer.
- Thumbnail viewer: Displays thumbnail of images to help view pictures quickly.
- Robust File System Analysis: Support for common file systems, including NTFS, FAT12/FAT16/FAT32/ExFAT, HFS+, ISO9660 (CD-ROM), Ext2/Ext3/Ext4, Yaffs2, and UFS from The Sleuth Kit.
- Hash Set Filtering: Filter out good known files using NSRL and flag bad known files using custom hashsets in HashKeeper, md5sum, and EnCase formats.
- Tags: Tag files with arbitrary tag names, such as 'bookmark' or 'suspicious', and add comments.
- Unicode Strings Extraction: Extracts strings from an unallocated space and unknown file types in many languages (Arabic, Chinese, Japanese, etc.).
- File Type Detection is based on detection of signatures and extension mismatch.
- Interesting Files Module will flag files and folders based on name and path.
- Android Support: Extracts data from SMS, call logs, contacts, Tango, Words with Friends, and more. (The Sleuth Kit, 2018)

Ingest Module usage

Ingest Module is a very helpful and powerful feature. During the initial case setup, it offers selection of needed ingest modules as shown in Figure 36. It identifies files and extracts known data as records. Examples of those records are emails, SMS messages, etc. Analysis of time and disk space may vary depending on how many modules are selected. It is important to have an Android Analyser module selected if an Android device image is an object of the import.

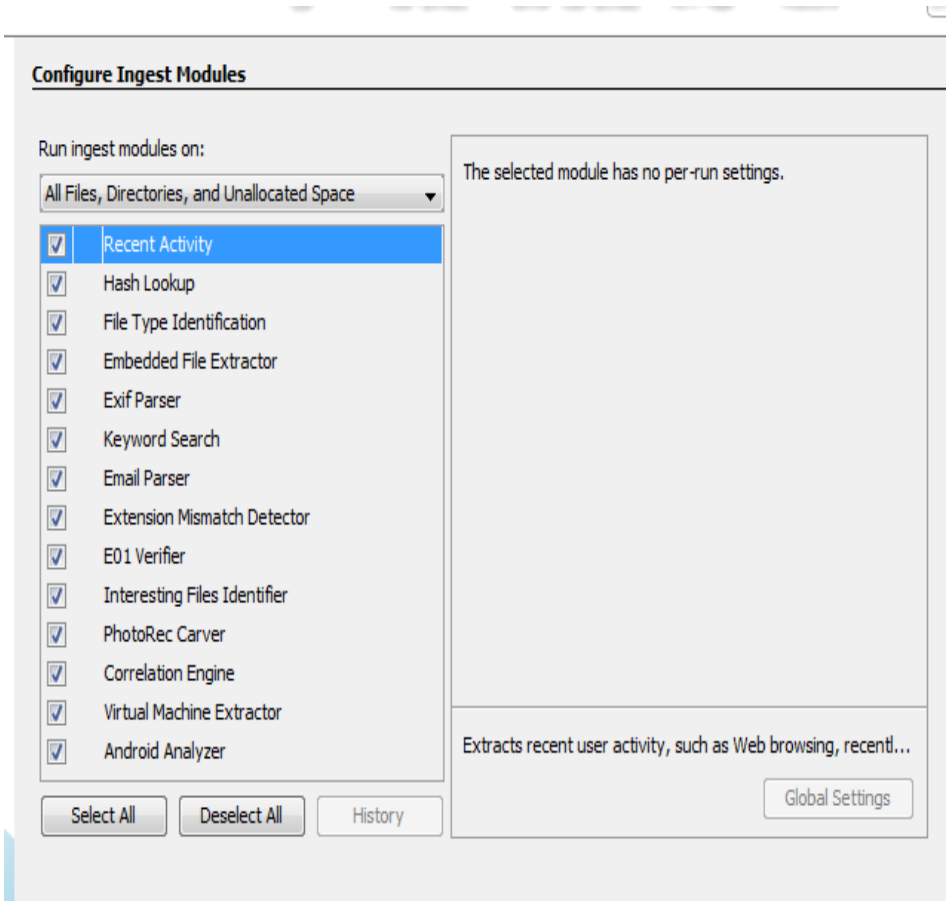


Figure 36. Autopsy Ingest Module

Android Analyser module usage

This module helps identify files and present data containing contacts, messages and other communications records, web history, web bookmarks etc. It gives an option to manually tag findings for different types of categories such as Child Exploitation. Figure 37. shows which types of categorization can be found on the main screen.

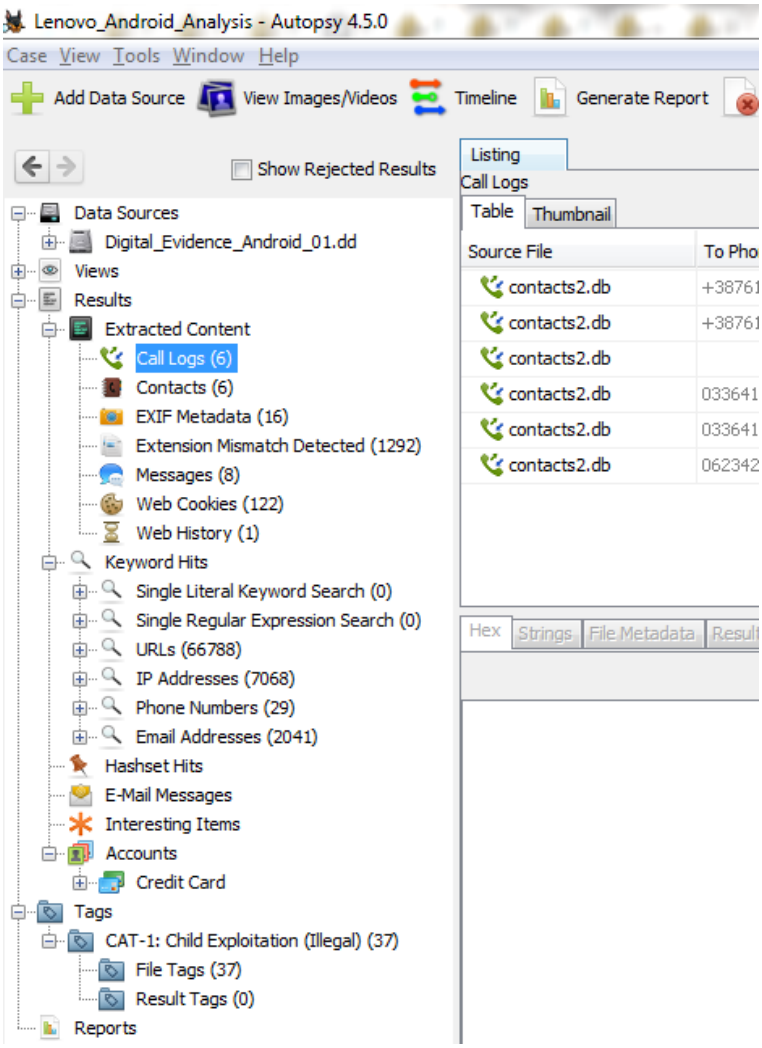


Figure 37. Android Analyzer

Accessing Partitions

Beside an automatic search for interesting records, it is possible to access image partitions manually. This offers another view to the acquired data, having a flexible approach to the offered data structure. Figure 38. shows all partitions acquired by the physical acquisition.

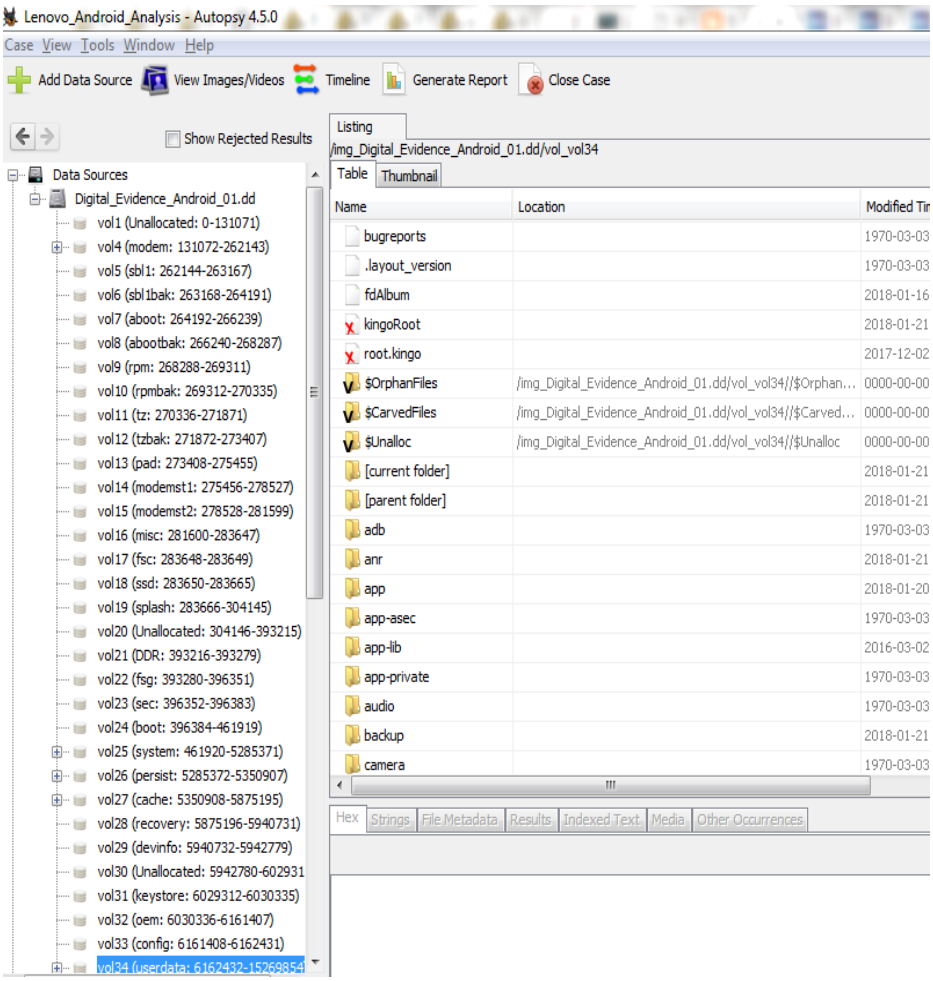


Figure 38. Access to Imaged Partitions

Timeline

Timeline option offers a powerful overview of the recorded events in time domain. With filtering options, timeline makes context building in View Mode Counts easier (Figure 39.).

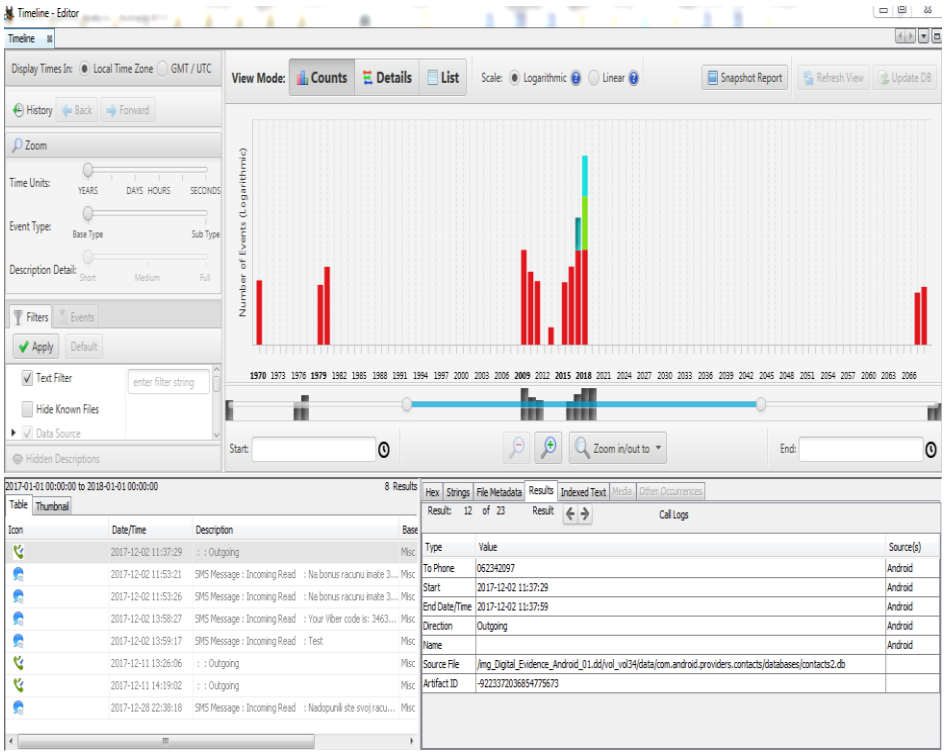


Figure 39. Timeline – View Counts

Colours represent main types of event categories, File System, Web Activity, and Misc. Types (Figure 40.). This filter is useful when many events are presented, thus allowing the focus on the interesting ones.

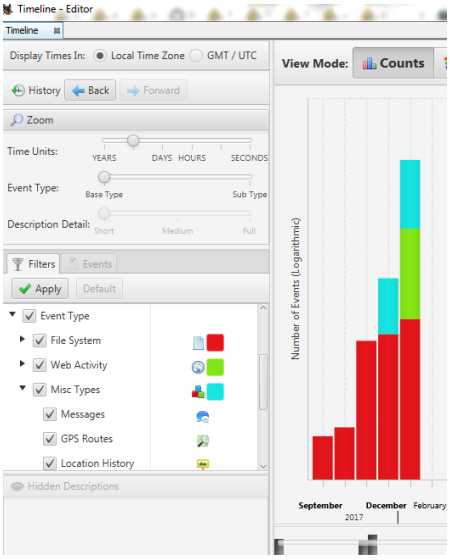


Figure 40. Filter Events Categories

When the View Mode is set to Details, it is possible to see and pin a potential interesting event. Figure 41. shows SMS and pinned messages.

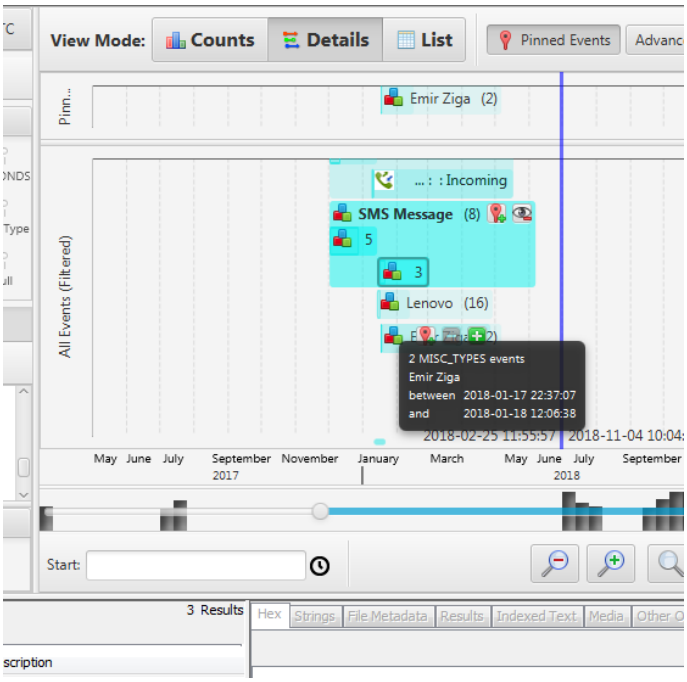


Figure 41. Timeline - View Details

Reporting

Autopsy offers an option of generating reports in various formats (Figure 42.). The final report will include either all analysis results or only tagged ones. When a large amount of data is generated, Excel format report gives more flexibility in case that data needs to be exported further.

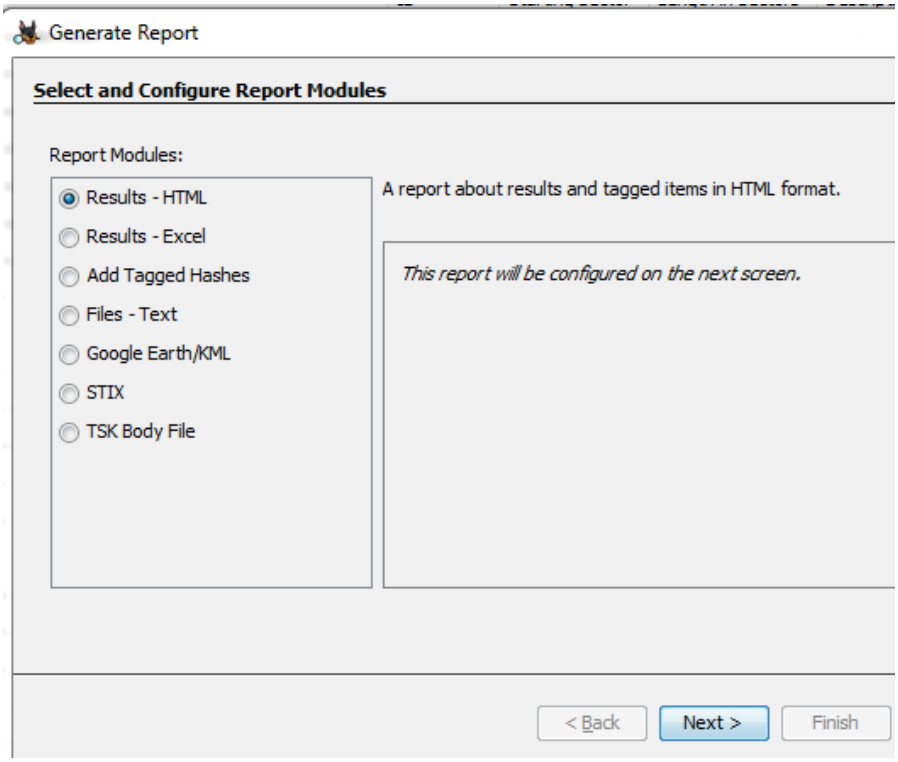


Figure 42. Report Formats

Generated report is filled with the case summary as shown in Figure 43.

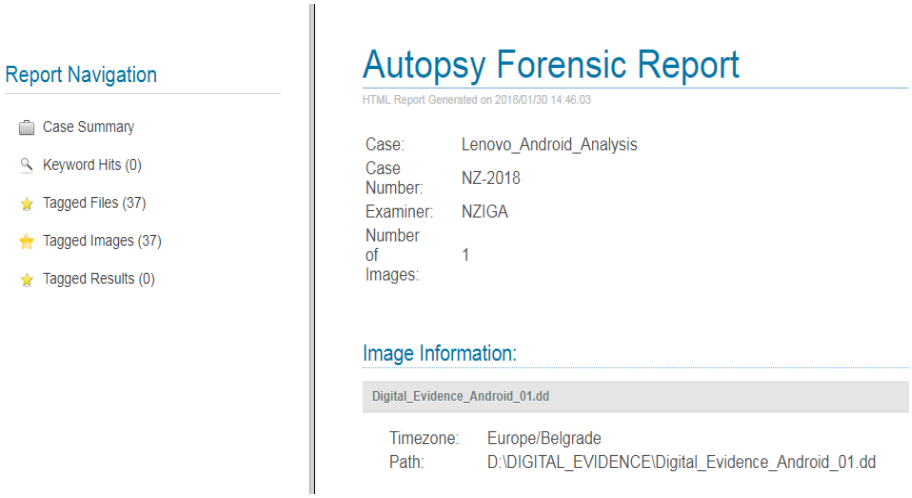


Figure 43. Report - Case Summary

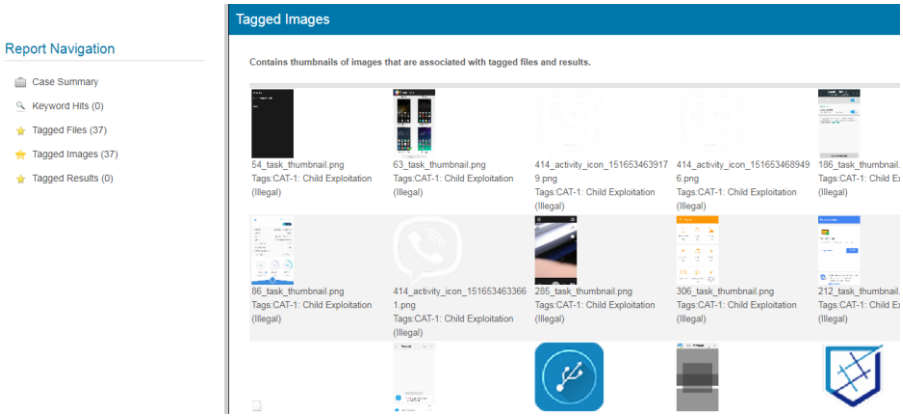


Figure 44. Report - Tagged Images

Figure 44. shows a detailed list of Keyword Hits, Tagged Files, Tagged Images, or Tagged Results.

Summary

Cyber security is a subset of information security which deals with the security of information stored in a digital form and transferred over

communication links. A great part of information security related standards deals with cyber security issues.

Almost daily, media reports reveal cyber security related incidents. After the historical analysis, we can conclude that we will see an increase in the frequency of incidents of this type, especially as more services and users use digital technology in their everyday work and life.

Knowledge acquired

Digital forensics – tools and usage: of hard disk and memory card docking stations, Portable Computer Forensic Lab, usage of general computer forensic tools such as

Disk Genius usage, DD command tool usage, Busybox usage. Database tools usage such as the Oracle LogMiner, IBM Guardium Data Protection for Databases, DB Browser for SQlite, Undark - a SQLite data recovery tool, SQLite-Deleted-Records-Parser. Usage of the network forensic tools such as Wireshark usage, NIKSUN NetDetector, Xplico usage. Usage of the mobile device forensic tools such as Rooting Tools usage, Santoku usage, Autopsy and the Sleuth Kit, Ingest Module usage, Android Analyser module and how to access partitions and use reports.

Review questions

1. Explain the difference between digital forensics tools.
2. Name tools for each technology?
3. Steps for mobile forensic investigation.

Further readings

- Digital transformation: online guide to digital business transformation

https://www.i-scoop.eu/digital-transformation/

- United States Secret Service:

Best Practices for Seizing Electronic Evidence

http://www.forwardedge2.usss.gov/pdf/bestPractices.pdf

- National Institute of Justice:

Forensic Examination of Digital Evidence: A Guide for Law Enforcement

https://www.ncjrs.gov/pdffiles1/nij/199408.pdf

- National Institute of Justice:

Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition

https://www.ncjrs.gov/pdffiles1/nij/219941.pdf

- National Institute of Justice:

Electronic Crime Scene Investigation: An On-the-Scene Reference for First Responders

https://www.ncjrs.gov/pdffiles1/nij/227050.pdf

- National Institute of Justice:

Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors

https://www.ncjrs.gov/pdffiles1/nij/211314.pdf

- Department of Justice:

Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations

- http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf

Video resources

- Disk Imaging/Acquisition Using Linux DD / DCFLDD command https://www.youtube.com/watch?v=aJp7_OVW2FA
- Computer Forensics: fdisk and dd https://www.youtube.com/watch?v=nzRo8gh7wkA
- Creating a Disk Image for Forensic Analysis https://www.youtube.com/watch?v=zY1rblisrBQ
- Starting a New Digital Forensic Investigation Case in Autopsy 4 https://www.youtube.com/watch?v=WB4xj8VYotk
- Processing and analysis of disk images with Autopsy 4 default modules https://www.youtube.com/watch?v=FJqoUakfmdo
- NIKSUN Netdetector https://niksun.com/notebook.php

5. Simulation of digital forensic cases

Chapter abstract

Chapter goals: To present digital forensic investigation cases which deal with the general computer, smart and mobile phones, and databases. To provide an insight into real forensic investigation processes not limited to single technology or a tool.

Learning outcomes: Knowledge of the possible ways in which digital forensic cases can be performed explained in different case simulated scenarios offering students a real hands-on experience from presented cases.

Case 1: Forensic data recovery of files on PC

The goal of the forensic investigation was to find a specific file on a disk on which windows quick-format was performed. There was no need to acquire live data for this process, because disk had already been removed from the PC.

For this purpose, Disk Genius was first used together with the hard disk docking station to clone the original disk to the investigation disk, and then to copy cloned data to the local investigator's forensic station.

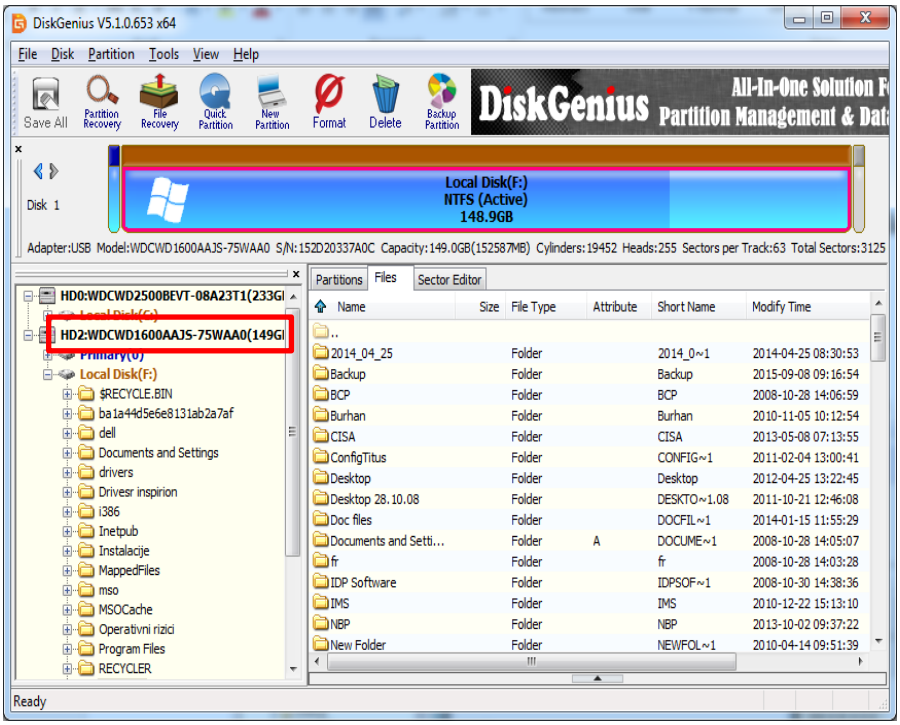


Figure 45. Disk Genius access to the investigated hard disk

Figure 46. shows how data was copied from the cloned hard disk to the local forensic investigator PC. All folders and files were available and needed file was easy to find.

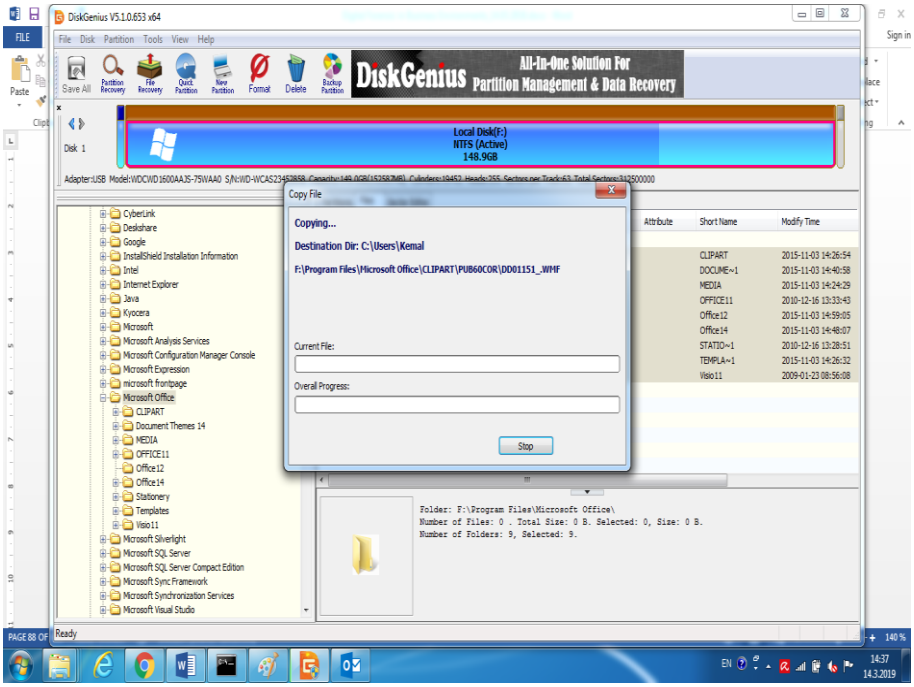


Figure 46. Disk Genius data copy

Case 2: Forensic investigation of Viber, VOICE CALL, SMS, and Coco on an Android mobile device

While working with the law enforcement team as contractors, we came across the case of two harassed persons. They were under the pressure because they were harassed over digital channels such as Global System for Mobile Communications (GSM) call, SMS text message, Viber message and threatening photographs, and Coco messenger. Both of them showed their Android smartphone devices with disturbing content. Everything was documented in the file.

Local police arrested the suspect and seized his Android mobile phone while following all the rules and procedures. The android mobile device was labelled and shielded against the radio frequency radiation, thus isolating the source of evidence, and transported to the laboratory.

Defining the Scope of the Investigation

Scope definition presents an important factor of the investigation. The initial interview with reporting persons discovered some basic information about events such as date and time, content, digital channel etc.

Seized device in this particular case was Lenovo A2020a40 running Android operating system version 5.1.1 equipped with GSM SIM card +38761078857. Device did not have any external storage, nor was it

locked or encrypted. USB debugging was enabled. Team collected all available information from the first victim (referred to as person 1).

TABLE 2. Reporting Person 1 Data

Report 061abcdef	Content	Date time of receipt
SMS message	Hi beauty, I saw you yesterday.	3.2.2018 15:23
Viber message	I'm in love with you.	2.2.2018 10:27
Viber photo	Picture of message "Are you afraid of the night?"	3.2.2018 15:29
Viber call		2.2.2018 10:31 duration 63 sec

Team also collected all available information from the second victim (referred to as person 2).

TABLE 3. Reporting Person 2 Data

Report 062342097	Content	Date time of receipt
GSM Voice call	-	2.12.2017 11:37 duration 30 seconds
Coco message	Careful with your door lock	3.2.2018 15:25
Coco message	You promised me not to leave me alone. Now you will regret.	2.2.2018 10:42

Both victims experienced unpleasant calls, messages, and photographs delivered over:

- Traditional voice GSM service
- Traditional SMS GSM service
- Viber Internet service
- Coco Internet service

First of all, it was necessary to search for the evidence on the seized Android device without knowing whether or not potential digital artefacts were deleted. After an additional analysis, decision was made to search for database files and photographs in both spaces – allocated and especially unallocated – because it was assumed that perpetrator deleted

all or some of the messages/calls/photographs. Goal was to find as much evidence as possible against the attacker.

Preparing the Environment for the Data Acquisition

Workstation dedicated for the investigation must be equipped with hardware and software needed for the image acquisition. Depending on the type of image data acquisition, some prerequisites must be met. Communication interface for the object of the investigation needs to be ADB connected over the USB port. Since this scope is limited to gathering logical images, some additional steps must be performed beforehand.

- Verifying ADB interface
- Root the device
- Install Busybox set of utilities

Verifying ADB Interface

The installed ADB connector will act as a link between the workstation and device, and it will be shown in a device manager as presented in Figure 47. If there is a malfunctioning issue, it will be shown at this point.

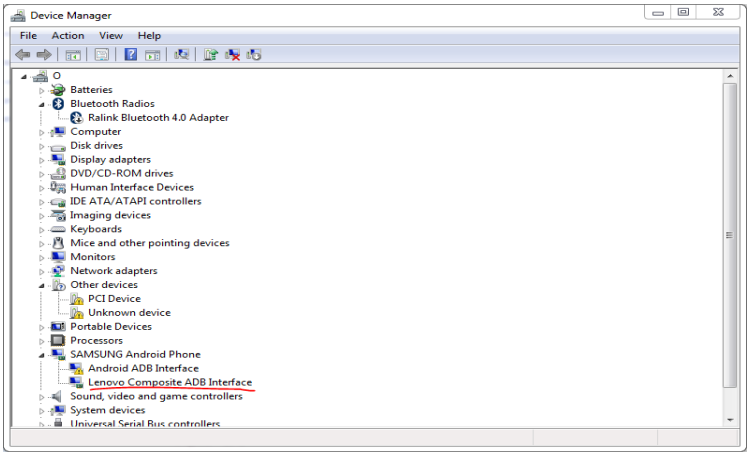


Figure 47. ADB Driver Verified; Android Device Connected

Rooting the Device

Device rooting is needed in order to obtain privileges for the full access to a system, or a non-volatile memory landscape. This step is critical to get root privileges for forensic activities. Process requires to:

- Connect device to USB
- Start the rooting tool

When the Android device is connected to the workstation, it will appear in a tray (Figure 48.), as well as in device manager under control panel.

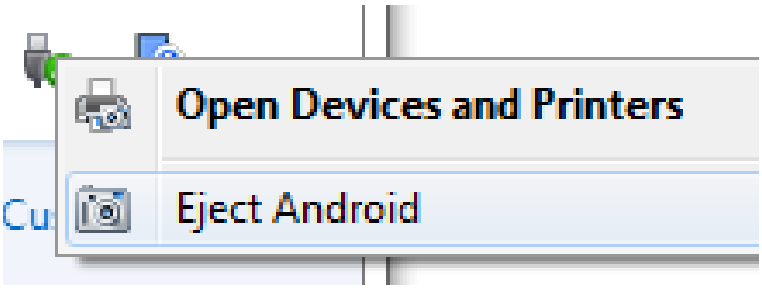


Figure 48. Android Device Connected

In order to check adb connection, it is necessary to start the command ADB DEVICES from the following location:

C:\Users\<username>\AppData\Local\Android\sdk\platform-tools

This is the location where platform tools with adb utility are installed. Figure 49. shows that workstation has been successfully communicated with the mobile device named 8d62f4b5.

```
C:\Users\tata\AppData\Local\Android\sdk\platform-tools>dir
 Volume in drive C has no label.
 Volume Serial Number is 2031-5DCE

 Directory of C:\Users\tata\AppData\Local\Android\sdk\platform-tools

09/04/2016  14:42    <DIR>          .
09/04/2016  14:42    <DIR>          ..
31/03/2016  15:03         1,419,776 adb.exe
31/03/2016  15:03            97,792 AdbWinApi.dll
31/03/2016  15:03            62,976 AdbWinUsbApi.dll
31/03/2016  15:03    <DIR>          api
31/03/2016  15:03            73,728 dmtracedump.exe
31/03/2016  15:03           338,944 etc1tool.exe
31/03/2016  15:03           319,488 fastboot.exe
31/03/2016  15:03            43,008 hprof-conv.exe
31/03/2016  15:03    <DIR>          lib64
31/03/2016  15:03           234,920 NOTICE.txt
09/04/2016  14:42            17,513 package.xml
31/03/2016  15:03            17,015 source.properties
31/03/2016  15:03           718,848 sqlite3.exe
31/03/2016  15:03    <DIR>          systrace
               11 File(s)      3,344,008 bytes
                5 Dir(s)  14,272,196,608 bytes free

C:\Users\tata\AppData\Local\Android\sdk\platform-tools>adb devices
List of devices attached
* daemon not running. starting it now on port 5037 *
* daemon started successfully *
8d62f4b5        device

C:\Users\tata\AppData\Local\Android\sdk\platform-tools>
```

Figure 49. Successful Communication to Mobile Device over ADB

Before using rooting tools, some precautions must be taken. Rooting is a powerful process and it can lead to a damage of phone and/or evidence. If the rooting process is used under normal circumstances, then it immediately leads to the warranty void. Antivirus and firewall setup can interfere with normal operations. Checking and testing connection should be done before the usage.

Starting tool for rooting will show the basic data. Introduction screen shows data about the device and the start button (Figure 50.). If the device is recognized, then the process can be initiated by pressing the “root” button.

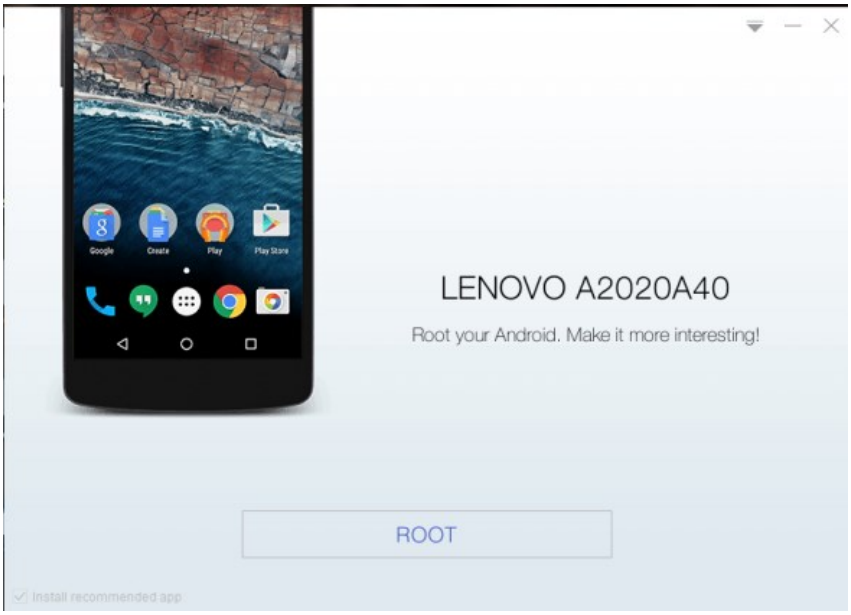


Figure 50. Lenovo Rooting Start

Progress will last for a couple of minutes and will be shown in the application. During the process, device screen will display the status of rooting (Figure 51.).

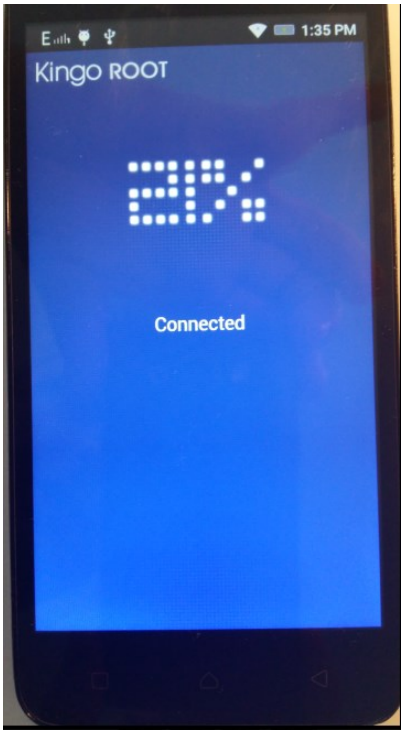


Figure 51. Device Status During Rooting Process

When the process is successfully completed, the message “succeed” will appear. Each brand has its own supporting software, but there are many other applications used for root checking, one of which is the RootChecker.

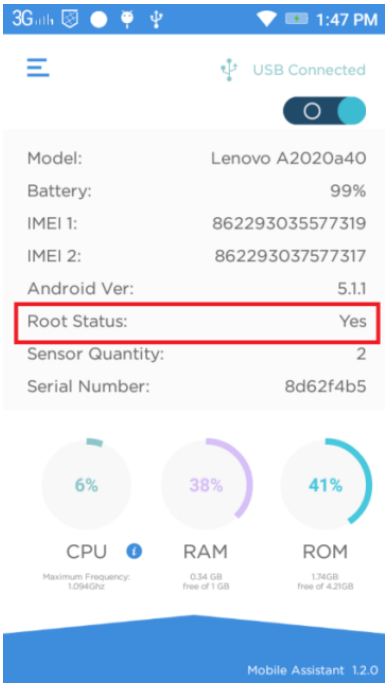


Figure 52. Lenovo Moto Smart Assistant Device Status

Lenovo Moto Smart Assistant was used to check the status of the device (Figure 52.).

Busybox Sideloading

Since Android is a Linux-based operating system, it is quite useful to have it installed on your device. After checking the adb connection to device, it is necessary to place the .apk busy box file (ru.meefik.busybox_34.apk) within the folder /android-sdk/platform-tools. Adb is available in the same location.

In order to sideload the application, run the following command in command line (Figure 53.):

Adb install ru.meefik.busybox_34.apk

```
C:\Users\tata\AppData\Local\Android\sdk\platform-tools>adb install ru.meefik.bus
ybox_34.apk
1653 KB/s (4323043 bytes in 2.553s)
        pkg: /data/local/tmp/ru.meefik.busybox_34.apk
```

Figure 53. Sideloading BusyBox Over ADB

In order to check if the installation was properly completed, type busybox in the device shell to see whether it starts (Figures 54, and 55.). Available commands will be listed.

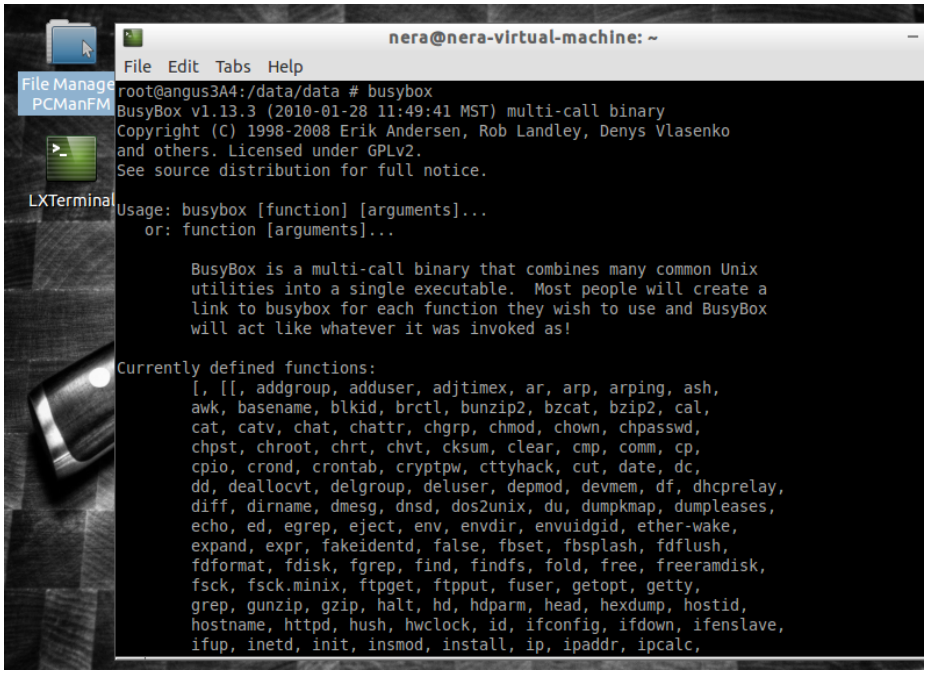


Figure 54. Starting Busybox

In order to use command SHA1SUM from Busybox toolset to calculate hash value of the file ueventd.rc, type #busybox sha1sum ueventd.rc (Figure 55.).

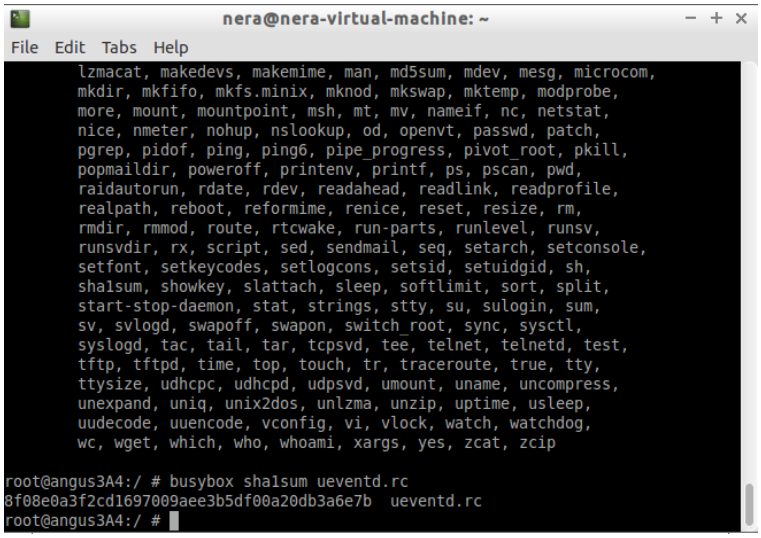


Figure 55. Testing Busybox Tool Sha1sum

Determining Partitions and Blocks

Since Android is a Linux-based operating system, partitions are organized in the same way as every other Linux OS. Knowledge of partitions, names, and mount points is necessary in order to get to the right place and determine the source of data before the imaging process begins. A simple command to list partitions is:

adb shell – to get to the andoid device
cat /proc/partitions

Running these commands will give an overview of what is happening on the partition level, thus, helping understand which block belongs to which partition name (Figure 56).

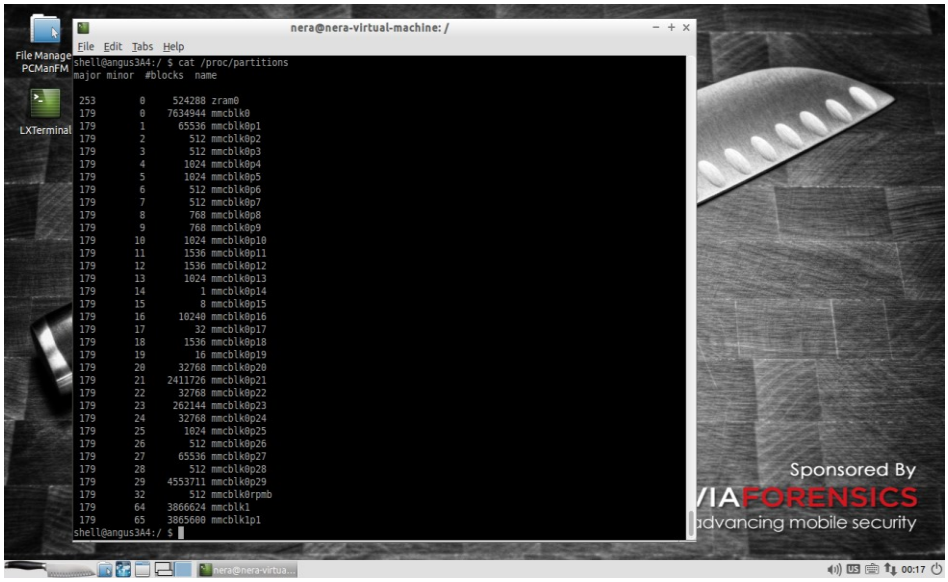


Figure 56. Android Block Names

Another way to obtain information about dev block names is adb shell

ls –la /dev/block/platform/7824900.sdhci/by-name

7824900.sdhci is not a common name for all devices, because it varies. It is also the subject of the investigation.

Running the command stated above will show results with more familiar names (Figure 57.).

During the imaging process it is important to decide which blocks will be captured and transferred. Usually a whole memory landscape (mmcblk0) is captured and transferred, however, in some special occasions only a single block might need imaging (e.g. mmcblk0p2). Names may vary, and they are subjects of device examination.

```
File  Edit  Tabs  Help

shell@angus3A4:/ $ ls -al /dev/block/platform/7824900.sdhci/by-name/
lrwxrwxrwx root     root              1970-02-28 22:58 DDR -> /dev/block/mmcblk0p17
lrwxrwxrwx root     root              1970-02-28 22:58 aboot -> /dev/block/mmcblk0p4
lrwxrwxrwx root     root              1970-02-28 22:58 abootbak -> /dev/block/mmcblk0p5
lrwxrwxrwx root     root              1970-02-28 22:58 boot -> /dev/block/mmcblk0p20
lrwxrwxrwx root     root              1970-02-28 22:58 cache -> /dev/block/mmcblk0p23
lrwxrwxrwx root     root              1970-02-28 22:58 config -> /dev/block/mmcblk0p28
lrwxrwxrwx root     root              1970-02-28 22:58 devinfo -> /dev/block/mmcblk0p25
lrwxrwxrwx root     root              1970-02-28 22:58 fsc -> /dev/block/mmcblk0p14
lrwxrwxrwx root     root              1970-02-28 22:58 fsg -> /dev/block/mmcblk0p18
lrwxrwxrwx root     root              1970-02-28 22:58 keystore -> /dev/block/mmcblk0p26
lrwxrwxrwx root     root              1970-02-28 22:58 misc -> /dev/block/mmcblk0p13
lrwxrwxrwx root     root              1970-02-28 22:58 modem -> /dev/block/mmcblk0p1
lrwxrwxrwx root     root              1970-02-28 22:58 modemst1 -> /dev/block/mmcblk0p11
lrwxrwxrwx root     root              1970-02-28 22:58 modemst2 -> /dev/block/mmcblk0p12
lrwxrwxrwx root     root              1970-02-28 22:58 oem -> /dev/block/mmcblk0p27
lrwxrwxrwx root     root              1970-02-28 22:58 pad -> /dev/block/mmcblk0p10
lrwxrwxrwx root     root              1970-02-28 22:58 persist -> /dev/block/mmcblk0p22
lrwxrwxrwx root     root              1970-02-28 22:58 recovery -> /dev/block/mmcblk0p24
lrwxrwxrwx root     root              1970-02-28 22:58 rpm -> /dev/block/mmcblk0p6
lrwxrwxrwx root     root              1970-02-28 22:58 rpmbak -> /dev/block/mmcblk0p7
lrwxrwxrwx root     root              1970-02-28 22:58 sbl1 -> /dev/block/mmcblk0p2
lrwxrwxrwx root     root              1970-02-28 22:58 sbl1bak -> /dev/block/mmcblk0p3
lrwxrwxrwx root     root              1970-02-28 22:58 sec -> /dev/block/mmcblk0p19
lrwxrwxrwx root     root              1970-02-28 22:58 splash -> /dev/block/mmcblk0p16
lrwxrwxrwx root     root              1970-02-28 22:58 ssd -> /dev/block/mmcblk0p15
lrwxrwxrwx root     root              1970-02-28 22:58 system -> /dev/block/mmcblk0p21
lrwxrwxrwx root     root              1970-02-28 22:58 tz -> /dev/block/mmcblk0p8
lrwxrwxrwx root     root              1970-02-28 22:58 tzbak -> /dev/block/mmcblk0p9
lrwxrwxrwx root     root              1970-02-28 22:58 userdata -> /dev/block/mmcblk0p29
shell@angus3A4:/ $
```

Figure 57. Android Partition Names and Blocks

Acquiring Data from the Evidence Device

Data from a device will be acquired by applying two methods, namely Physical and Logical data acquisition.

Logical data acquisition

To start the acquisition, Android device must have a debugging option enabled, and working adb. From the Linux command line start the command: aflogical-ose and then enter sudo password (Figure 58.).

```
nera@nera-virtual-machine: ~
File  Edit  Tabs  Help
nera@nera-virtual-machine:~$ aflogical-ose
Make sure android device is connected to USB
[sudo] password for nera:

414 KB/s (28794 bytes in 0.067s)
        pkg: /data/local/tmp/AFLogical-OSE_1.5.2.apk
```

Figure 58. Starting AFLogical OSE acquisition

Before pressing Enter to pull data on the device, it is necessary to mark interesting logs for acquisition, and then press the "capture" button (Figure 59.).

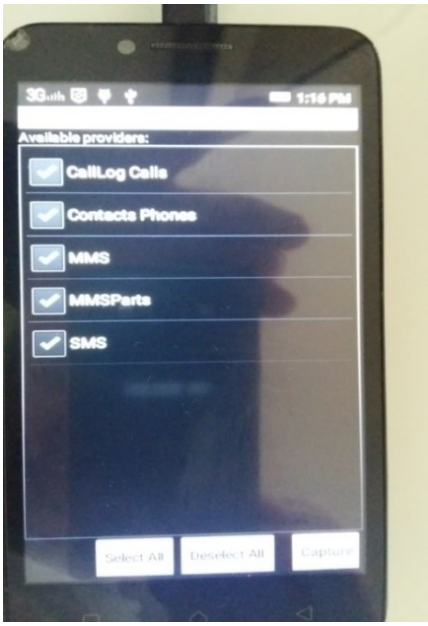


Figure 59. Device Capture Options

Data is transferred to the remote folder with data packed in a comma separated value format (Figure 60).

```
nera@nera-virtual-machine: ~
File  Edit  Tabs  Help
Starting: Intent { cmp=com.viaforensics.android.aflogical_ose/com.viaforensics.a
ndroid.ForensicsActivity }

Press enter to pull /sdcard/forensics into ~/aflogical-data/

pull: building file list...
pull: /sdcard/forensics/20180117.2249/SMS.csv -> /home/nera/aflogical-data/20180
117.2249/SMS.csv
pull: /sdcard/forensics/20180117.2249/MMSParts.csv -> /home/nera/aflogical-data/
20180117.2249/MMSParts.csv
pull: /sdcard/forensics/20180117.2249/Contacts Phones.csv -> /home/nera/aflogica
l-data/20180117.2249/Contacts Phones.csv
pull: /sdcard/forensics/20180117.2249/MMS.csv -> /home/nera/aflogical-data/20180
117.2249/MMS.csv
pull: /sdcard/forensics/20180117.2249/CallLog Calls.csv -> /home/nera/aflogical-
data/20180117.2249/CallLog Calls.csv
pull: /sdcard/forensics/20180117.2249/info.xml -> /home/nera/aflogical-data/2018
0117.2249/info.xml
pull: /sdcard/forensics/20180203.1316/Contacts Phones.csv -> /home/nera/aflogica
l-data/20180203.1316/Contacts Phones.csv
pull: /sdcard/forensics/20180203.1316/MMS.csv -> /home/nera/aflogical-data/20180
203.1316/MMS.csv
pull: /sdcard/forensics/20180203.1316/SMS.csv -> /home/nera/aflogical-data/20180
203.1316/SMS.csv
pull: /sdcard/forensics/20180203.1316/CallLog Calls.csv -> /home/nera/aflogical-
data/20180203.1316/CallLog Calls.csv
pull: /sdcard/forensics/20180203.1316/MMSParts.csv -> /home/nera/aflogical-data/
20180203.1316/MMSParts.csv
pull: /sdcard/forensics/20180203.1316/info.xml -> /home/nera/aflogical-data/2018
0203.1316/info.xml
12 files pulled. 0 files skipped.
```

Figure 60. AFLogical OSE Data Extraction and Transfer

Acquired data can be found in folder /home/nera/aflogical-data/ (Figure 61).

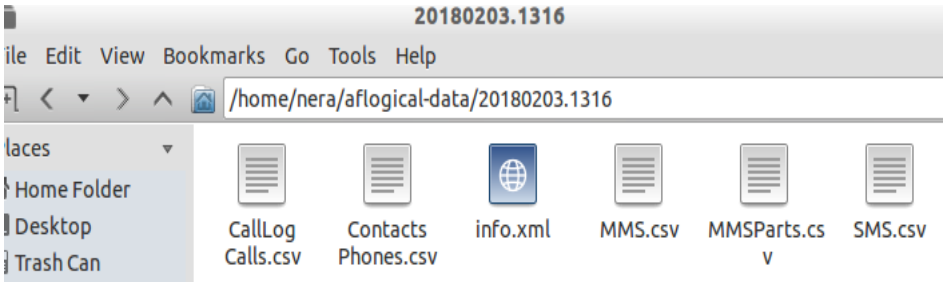


Figure 61. Acquired Data in Remote Folder

Data in this folder shows only what logically exists in the phone records regarding logs we were offered, and which we selected during the initial logical acquisition step. Deleted records are not available.

Physical data acquisition

In this process, the imaging command of the /dev/block will be issued and at the same time the transfer over adb link using redirection will be initiated. Netcat utility will allow forwarding commands across the adb link.

For the imaging process, Linux command dd will be used. Syntax is:

```
dd if=/mountpoint of=/destinationpoint/partitiontype
of – Output can be redirected thru netcat (nc) to remote file
dd if=/mountpoint | busybox nc –l –p portnumber
```

Obtaining data from the source device will be done through two opened concurrent shells in Santoku investigative workstation (Figure 62.). This process can take some time. In this case, 7818182656 bytes were transferred in 7836.341 seconds (approximately 130 minutes).

Remote destination should have enough storage to receive an image. Another important factor is the type of file system being formatted. FAT32 will not be able to accept a file larger than 4GB.

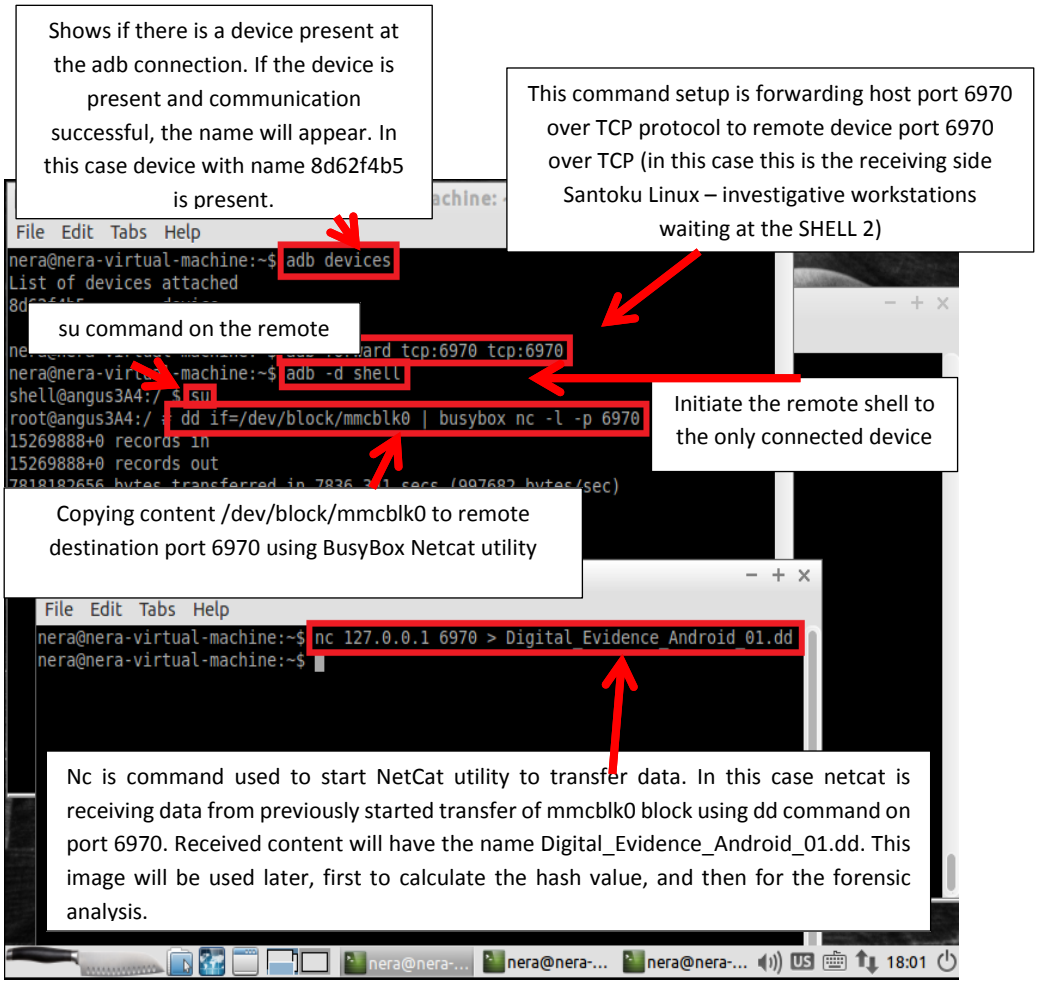


Figure 62. An integrity of the evidence image file

In order to maintain integrity check of the obtained image file, hash calculation has to be performed and documented (Figure 63.). Calculated hash value is checked through the entire process, and complete life cycle of evidence.

Command issued in the shell is:

Sha256sum Digital_Evidence_Android_01.dd

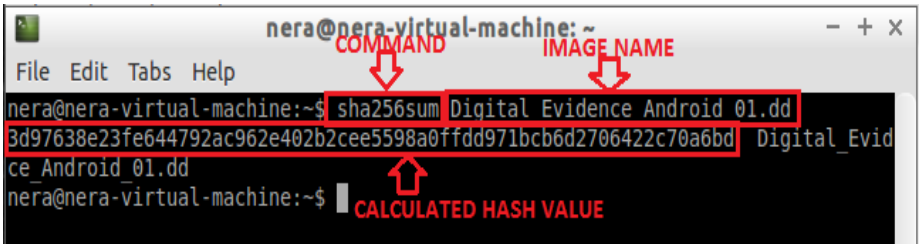


Figure 63. Calculating Hash Value of the Evidence Image

Importing Image File into Autopsy

Before the analysis starts, collected image file needs to be imported into tool Autopsy 4.5.0. This process can take a while depending on a size of the image file. During the image collection process, dd command is used to collect the whole image of Android device including unallocated space for allowing a deeper analysis. During the initial case creation, option Disk Image or VM File was chosen as a data source. Ingestion module is left with default settings fully marked with all available options.

Analysis of the Acquired Mobile Device Data

Data acquired with both methods logical and physical will be the subject of the investigation.

Analysis of Logically Acquired Data

Logical acquisition is simple, and all data acquired from the phone is located in one folder with names which correspond to data (Figure 64).

CallLog Calls.csv	03/02/2018 13:21	Microsoft Excel C...	1 KB
Contacts Phones.csv	03/02/2018 13:21	Microsoft Excel C...	1 KB
info.xml	03/02/2018 13:21	XML Document	146 KB
MMS.csv	03/02/2018 13:21	Microsoft Excel C...	1 KB
MMSParts.csv	03/02/2018 13:21	Microsoft Excel C...	1 KB
SMS.csv	03/02/2018 13:21	Microsoft Excel C...	3 KB

Figure 64. Files Containing Acquired Data

Figure 65. shows the content of the file SMS.csv.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
_id	thread_id	address	person	date	date_sent	protocol	read	status	type	rep	subject	body	service_cer	locked
10	5	+387 61 139 669		1516641841878	0		1	-1	2			I have to be with you.		0
9	3	+387 62 342 097		1516634801041	0		1	-1	2			Test back		0
8	16	Facebook		1516366697036	1516366685000	0	1	-1	1	0		.. . . ` 's your Messenger confirmation code	4.673E+10	0
7	15	611171		1516273799512	1516273747000	0	1	-1	1	0		Dobili ste dopunu u iznosu 7KM od MojaTv korisnika NE	3.876E+10	0
6	5	38761139669		1515927039926	1515927036000	0	1	-1	1	0		Hi, get on Coco. It's awesome! http://d.icoco.com - and	3.876E+10	0
5	4	eUltra		1514497098107	1514497095000	52	1	-1	1	0		Nadopunili ste svoj racun sa 2.00 KM na datum 28.12.20	3.876E+10	0
4	3	38762342097		1512219557232	1512219518000	0	1	-1	1	0		Test	3.876E+10	0
3	2	Viber		1512215907267	1512215902000	0	1	-1	1	0		Your Viber code is:	3.203E+11	0
2	1	1204		1512212006828	1512211081000	2	1	-1	1	0		Na bonus racunu imate 3KM i 300MB. Vise informacija c	3.876E+10	0
1	1	1204		1512212001907	1512211081000	2	1	-1	1	0		Na bonus racunu imate 3KM i 300MB. Vise informacija c	3.876E+10	0

Figure 65. Content of SMS File

CallLog Calls.csv file contains data about calls. Corresponding records are found in the listing. Figure 66. shows that call is made to number 062342097, date is formatted as EPOCH [2] date time format, and 1512211049405 is 2.12.2017 11:37:29.405., with duration of 30 seconds.

_id	number	date	duration	type	new
1	62342097	1512211049405	30	2	0
4	33641085	1512995166488	0	2	0
5	33641085	1512998342750	48	2	0
6	38761286751	1515508789367	7	1	0
7	38761826602	1516225027315	0	2	0
8	38761826602	1516273597920	0	2	0
15	61321321	1517563429505	0	2	0
16	61139669	1517565326337	11	2	0

Figure 66. Content of CallLog Calls File

[2] The Unix epoch (or Unix time or POSIX time or Unix timestamp) is the number of seconds that have elapsed since January 1, 1970 (midnight UTC/GMT).

None of the other applications' log data was retrieved during the logical acquisition using AF Logical OSE tool. Other matches except voice call were found (Table 3. and Table 4.).

TABLE 4. Overview of Logically Acquired Data for Reporting Person 1

Report 061abcdef	Content	Date/time of receipt	Evidence/Logical acquisition found
SMS message	Hi beauty, I saw you yesterday.	3.2.2018 15:23	**NO**
Viber message	I'm in love with you.	2.2.2018 10:27	**NO**
Viber call		2.2.2018 10:31 call duration 1:03 sec	**NO**
Viber threating photo	Picture of the message "Are you afraid of the night?"	3.2.2018 15:29	**NO**

TABLE 5. Overview of Logically Acquired Data for Reporting Person 2

Report 062342097	Content	Date/time of receipt	Evidence/Logical acquisition found
GSM Voice call	-	2.12.2017 11:37 duration 30 seconds	**YES**
Coco message	Careful with your door lock	3.2.2018 15:25	**NO**
Coco message	You promised me not to leave me alone. Now you will regret.	2.2.2018 10:42	**NO**

Analysis of the Physically Acquired Data

Physical analysis begins with the Autopsy tool first. Full Android mobile device image Lenovo_Android05 is imported and ingest module runs on data with task configured at the beginning. Autopsy also searches unallocated space. It could particularly be interesting in case of hiding data or recovering deleted data.

Autopsy mounted 35 partitions (Figure 67.). Partition vol34 – userdata is the place where all applications hold data.

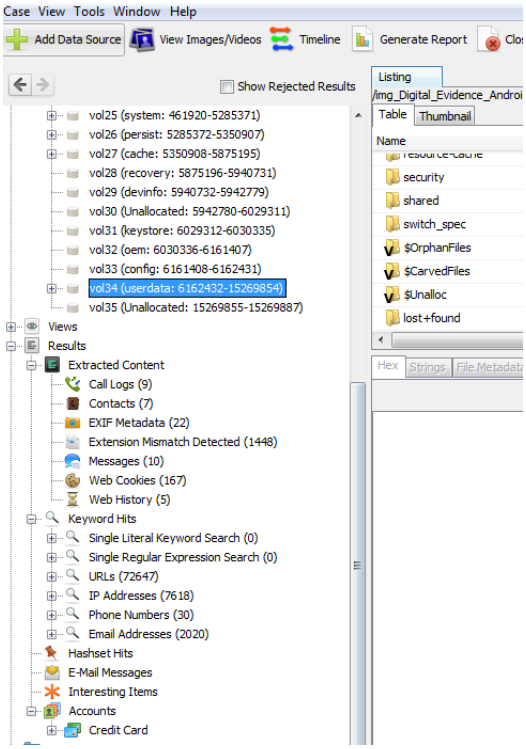


Figure 67. Autopsy Mounted Partition from the Evidence Image

Table 6. lists collected information about applications in the scope of investigation.

TABLE 6. Collected Data about Applications in Investigation Scope

Application name	Location of application	Location of database	Database names
Viber	/data/com.viber.voip	/data/com.viber.voip/databases	Viber_messages
SMS	/data/com.android.providers/telephony	/data/com.android.providers/telephony/databases	Mmssms.db
Coco msg/voice	/data/com.instanza.cocovoice	/data/com.instanza.cocovoice/databases	59317329_coco.db
GSM Telephone dialler	/data/com.android.providers.contacts	/data/com.android.providers.contacts/databases	Contacts2.db

Viber Message and Call Investigation

Viber investigation searched for evidence to match data from the table from the beginning of the case. The goal was to prove the existence of digital trail related to Viber. Table 7. shows receiving report from user 061abcdef.

TABLE 7. Viber Message and Call Investigation

Report 061abcdef	Content	Date/time of receipt
Viber message	I'm in love with you.	2.2.2018 10:27
Viber call		2.2.2018 10:31 call duration 1:03 sec
Viber threating photo	Picture of message "Are you afraid of the night?"	3.2.2018 15:29

First of all, we need to locate the proper partition and data path, found in the Viber database (Figure 68.).

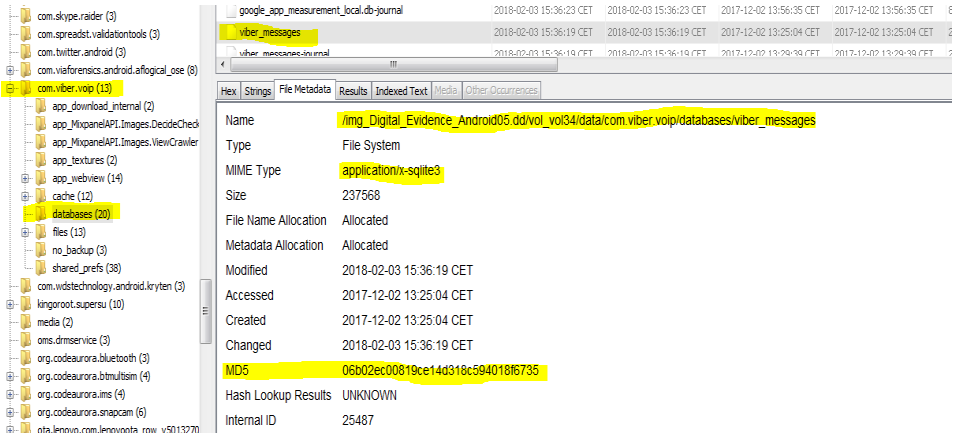


Figure 68. Viber Database Location and Metadata

Searching for the Viber Message – "I'm in love with you"

In order to find the message, database needs to be extracted to the operation folder (right click on database – extract) and then opened in DB Browser for SQLite.

Viber database structure is shown in Figure 69. Tables messages and messages_calls will be the subject of analysis because they contain data interesting for the investigation.

Database Structure | Browse Data | Edit Pragmas | Execute SQL

Create Table | Create Index | Modify Table | Delete Table

Name	Type	Schema
Tables (17)		
adx		CREATE TABLE adx (_id INTEGER PRIMARY KEY NOT NULL, event_name TEXT, last_tracked
applications		CREATE TABLE applications (_id INTEGER PRIMARY KEY NOT NULL, name TEXT, type TEXT
backgrounds		CREATE TABLE backgrounds (_id INTEGER PRIMARY KEY NOT NULL, background_index INT
blocked_data		CREATE TABLE blocked_data (_id INTEGER PRIMARY KEY AUTOINCREMENT, type INTEGER,
conversations		CREATE TABLE conversations (_id INTEGER PRIMARY KEY autoincrement,conversation_type
group_delete_all_from_participant		CREATE TABLE group_delete_all_from_participant (_id INTEGER PRIMARY KEY AUTOINCREM
messages		CREATE TABLE messages (_id INTEGER PRIMARY KEY autoincrement,address TEXT NOT NU
messages_calls		CREATE TABLE messages_calls (_id INTEGER PRIMARY KEY AUTOINCREMENT,conversation
messages_likes		CREATE TABLE messages_likes (_id INTEGER PRIMARY KEY AUTOINCREMENT,message_tok
participants		CREATE TABLE participants (_id INTEGER PRIMARY KEY autoincrement,conversation_id INT
participants_info		CREATE TABLE participants_info (_id INTEGER PRIMARY KEY autoincrement,number TEXT,e
public_accounts		CREATE TABLE public_accounts (_id INTEGER PRIMARY KEY autoincrement,group_id INTEG
purchase		CREATE TABLE purchase (order_id TEXT PRIMARY KEY NOT NULL, category INTEGER, type
remote_banners		CREATE TABLE remote_banners (_id INTEGER PRIMARY KEY AUTOINCREMENT, token LONG
sqlite_sequence		CREATE TABLE sqlite_sequence(name,seq)
stickers		CREATE TABLE stickers (_id INTEGER PRIMARY KEY NOT NULL, package_id INTEGER DEFAU
stickers_packages		CREATE TABLE stickers_packages (_id INTEGER PRIMARY KEY NOT NULL, package_info TEX
Indices (31)		
Views (0)		
Triggers (5)		

Figure 69. Viber Database Structure

Executing an SQL command over the table messages in database viber_message will yield results which is proof that the message “I’m in love with you” was sent from the phone (Figure 70.). Epoch data 1517563641920 is 2.2.2018 10:27:21.920

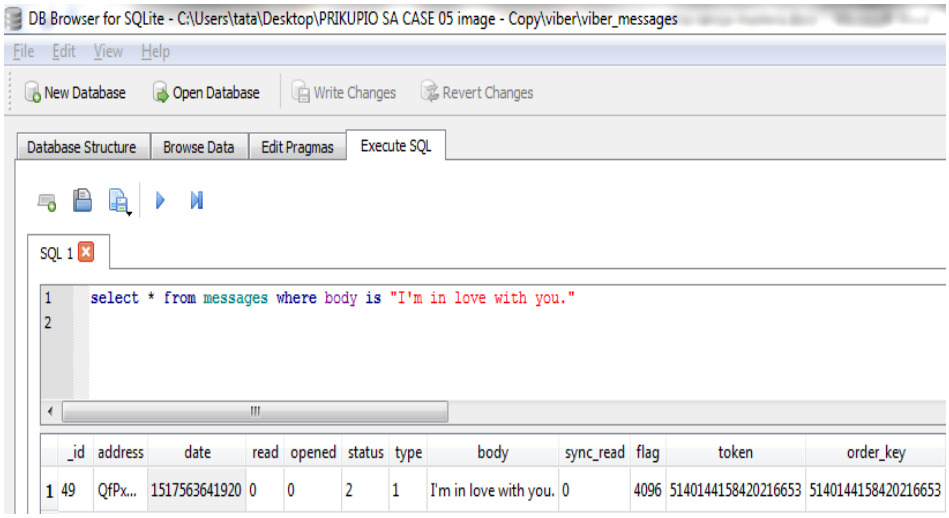


Figure 70. Retrieve Data About Message from Table Messages

Searching for the call 2.2.2018 10:31; call duration 1:03 sec

The following step is to find the trail for Viber call to 061abcdef on 2.2.2018 at 10:31; call duration 1:03 sec. Table message_calls contains data. Executing an SQL command with parameters needed to narrow query will return data which is a proof that the call was made from this phone (Figure 71). Epoch time 1517563892604 is equal to 2.2.2018 10:31:32.604.

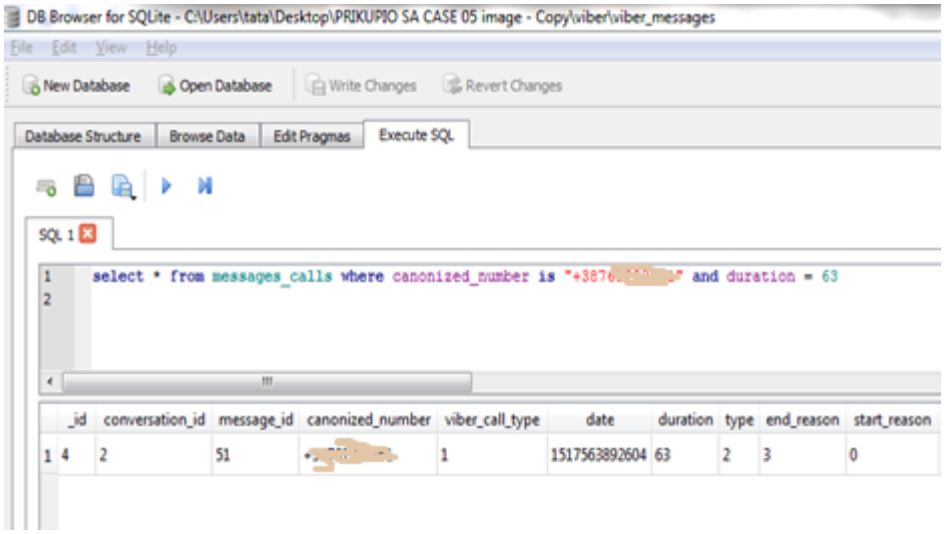


Figure 71. Retrieve Data About Calls from Table Messages_Calls

Searching for the sent picture of the message "Are you afraid of the night?"

The following task is to find the Viber picture/photo of the threatening message "Are you afraid of the night?" sent 3.2.2018 at 15:29.

Table messages in viber_messages database shows the record of a deleted message (Figure 72.).

Other than date/time value and status of the message, other available data is not in the scope of the investigation.

50		QfPxX...	1517563892604	0	0	2	1	outgoing_call	0	0	514014517...	51401451704...	0
51		QfPxX...	1517565117821	0	0	2	0	I'll call you later.	0	4096	514015034...	51401503459...	0
52		QfPxX...	1517565792930	0	0	2	0	incoming_call	0	0	514015314...	51401531426...	0
53		QfPxX...	1517566198804	0	0	2	1	file:///storage/sdc...	0	4096	514015494...	51401549450...	0
54		QfPxX...	1517667999674	0	0	2	1	message_deleted...	0	4096	514058187...	51405818750...	0
55		QfPxX...	1517668146820	0	0	2	1	message_deleted...	0	4096	514058258...	51405825845...	0

Figure 72. Viber Database Records

Epoch 1517668146820 is 3.2.2018 15:29:06.820 which corresponds to date and time from the initial search table. Another step is to search unallocated space for deleted pictures. Autopsy has a strong engine inspecting files according to the ingest module configuration. Picture was found as a deleted file (Figure 73.).

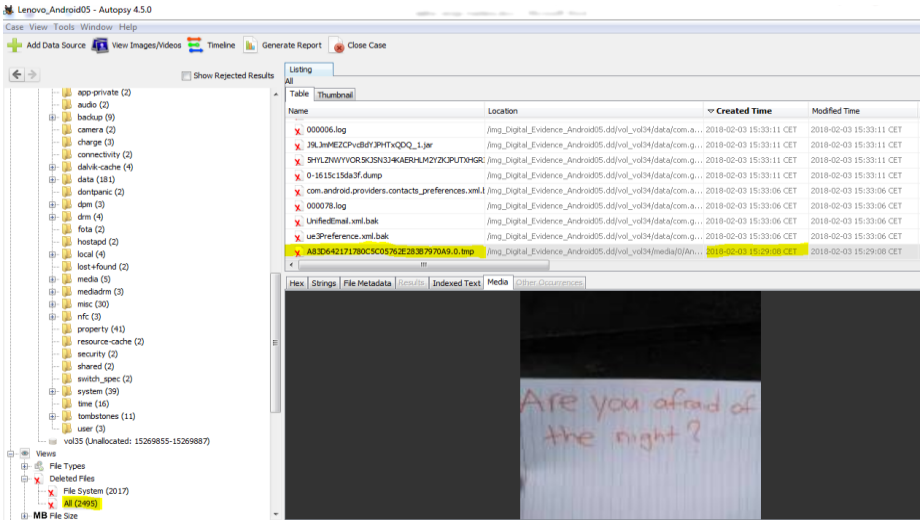
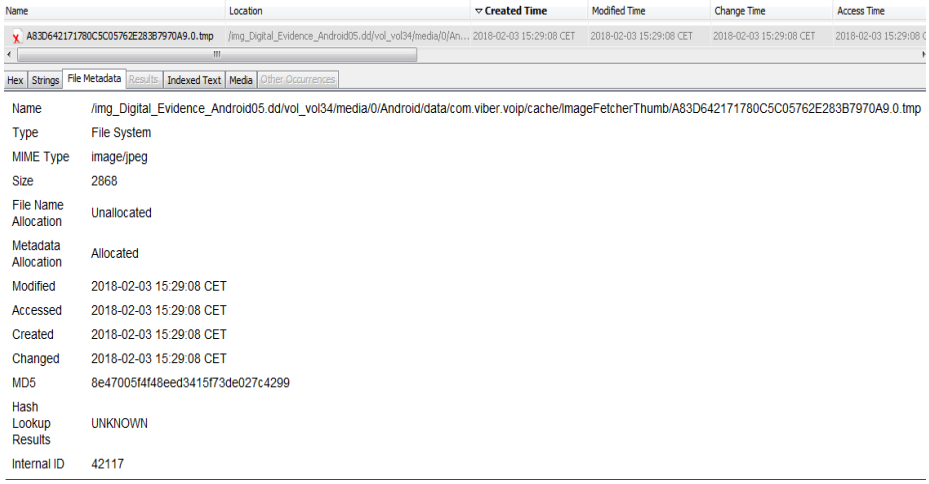


Figure 73. Recovered Deleted Picture

Additional data about the file is shown in Figure 74.



Name	Location	Created Time	Modified Time	Change Time	Access Time
A83D642171780C5C05762E283B7970A9.0.tmp	/img_Digital_Evidence_Android05.dd/vol_vol34/media/0/An...	2018-02-03 15:29:08 CET	2018-02-03 15:29:08 CET	2018-02-03 15:29:08 CET	2018-02-03 15:29:08 C

Hex | Strings | File Metadata | Results | Indexed Text | Media | Other Occurrences

Name	/img_Digital_Evidence_Android05.dd/vol_vol34/media/0/Android/data/com.viber.voip/cache/ImageFetcherThumb/A83D642171780C5C05762E283B7970A9.0.tmp
Type	File System
MIME Type	image/jpeg
Size	2868
File Name Allocation	Unallocated
Metadata Allocation	Allocated
Modified	2018-02-03 15:29:08 CET
Accessed	2018-02-03 15:29:08 CET
Created	2018-02-03 15:29:08 CET
Changed	2018-02-03 15:29:08 CET
MD5	8e47005f4f48eed3415f73de027c4299
Hash Lookup Results	UNKNOWN
Internal ID	42117

Figure 74. Recovered Deleted Picture Metadata

SMS Message Investigation

The scope of this investigation is database where SMS messages are stored. Initial data we were searching for is shown in Table 8.

TABLE 8. SMS Message Investigation

Report 061abcdef	Content	Date/time of receipt
SMS message	Hi beauty, I saw you yesterday.	3.2.2018 15:23

According to the previous mapping of the application location, SMS messages are stored in database mmssms.db located in /data/com.android.providers/telephony/databases. After the process of database extraction to the operational folder, the examination of the database structure is performed (Figure 75). Table named sms should have data about messages. Other tables were opened, and attributes were checked. Depending on the scope of the investigation, some other tables can be subject to a detailed analysis.

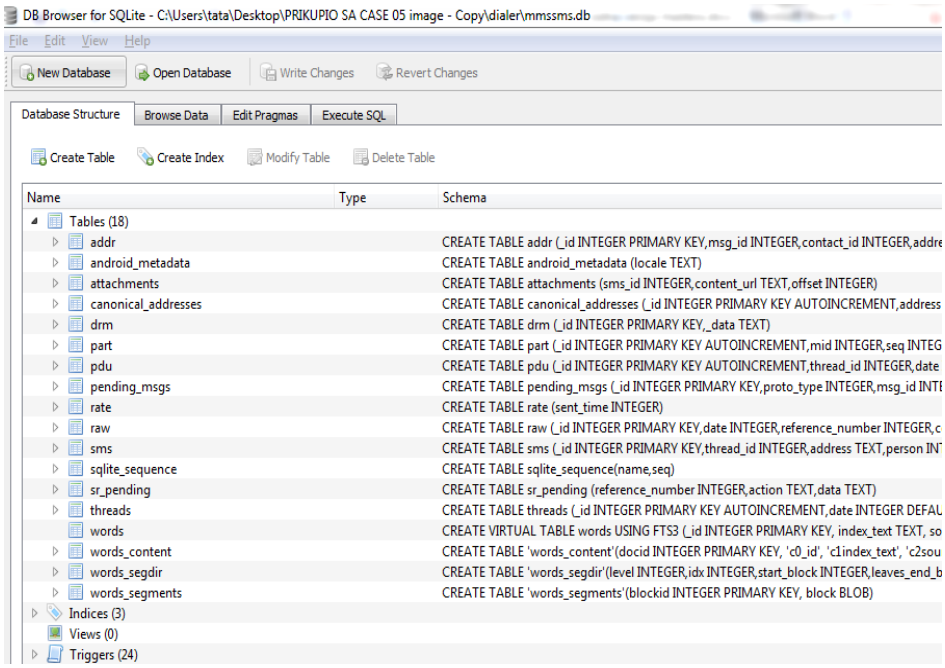


Figure 75. MMSSMS Database Structure

Searching for the sms message "Hi beauty, I saw you yesterday"

No other tables except the sms table contained the needed records. The investigation shows that records in table sms do not contain data about the message "Hi beauty, I saw you yesterday" (Figure 76.). It is assumed that the message is deleted from the database because executed SQL commands do not retrieve any data on setup condition. Other tools should be used to perform the possible data recovery at database level.

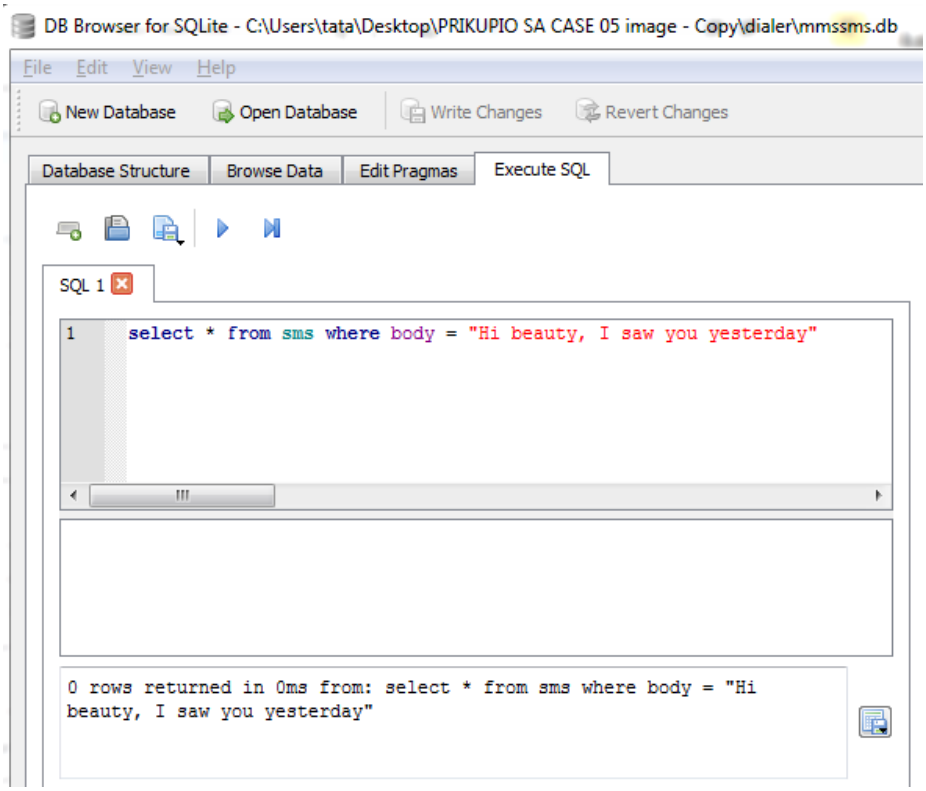


Figure 76. Retrieve Data about Calls from Table SMS

SQLite-Deleted-Records-Parser tool could help determine deleted data in database. Start tool with mmssms.db and output file mmssms.txt. After that, the execution message is found in unallocated space (Figure 77.).

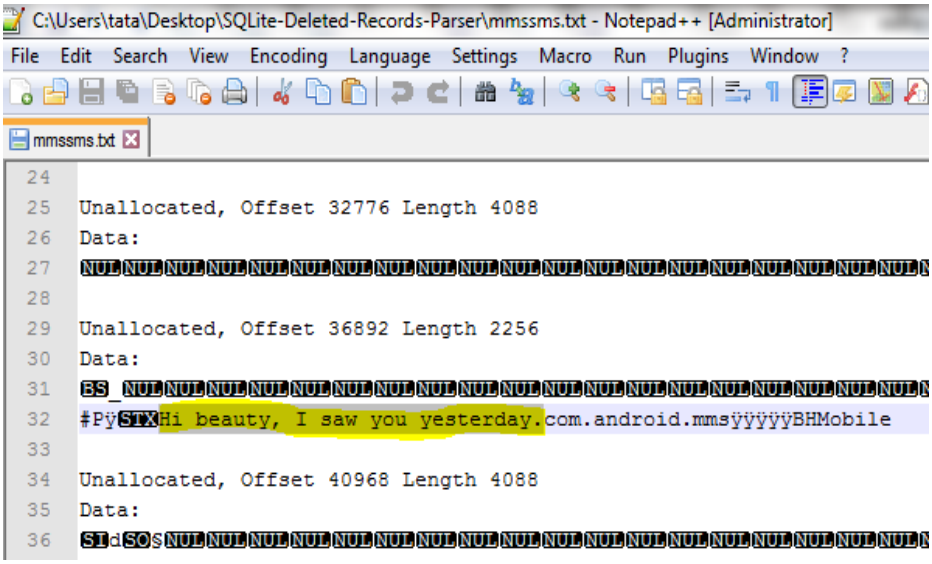


Figure 77. Recovered Deleted Database Record

GSM Voice Call Investigation

The scope of the GSM voice call investigation will be database where data records are stored. Initial data we were searching for is shown in Table 9.

TABLE 9. GSM Voice Call Investigation

Report 062342097	Content	Date time of receipt
GSM Voice call	-	2.12.2017 11:37 duration 30 seconds

Voice call log records can be found in database contact2.db located in /data/com.android.providers.contacts/databases. The structure of database after the extraction to the operational folder is shown in Figure 78.

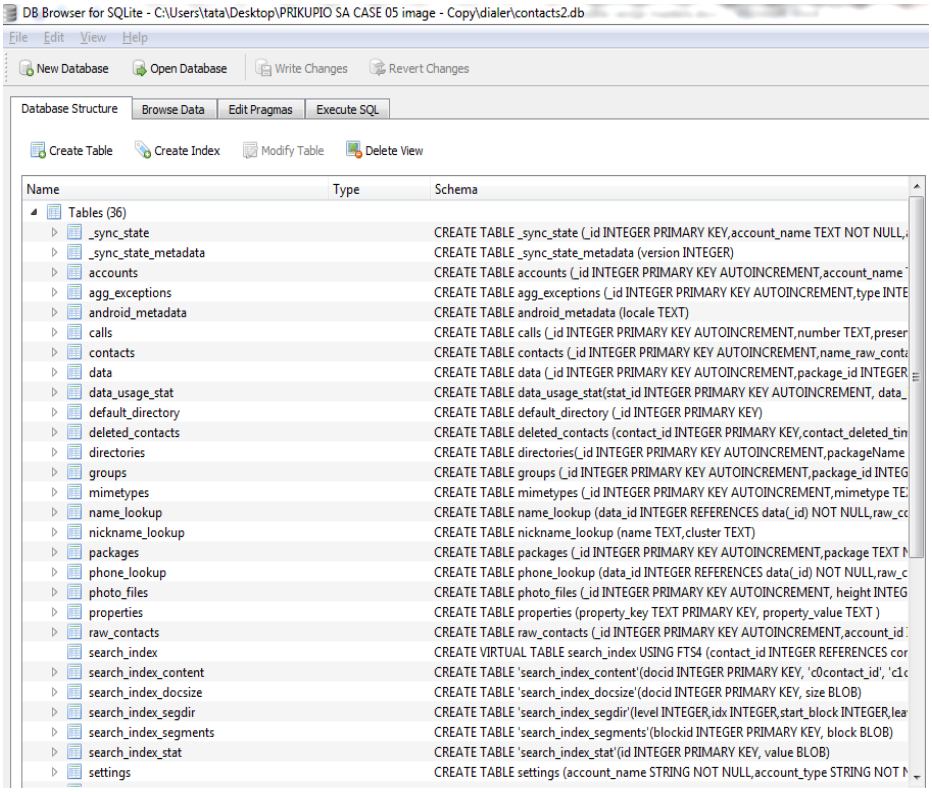


Figure 78. Contact2 Database Structure

Searching for the GSM voice call 2.12.2017 11:37 duration 30 seconds

Table calls should have data related to executed call, incoming as well as outgoing call. Executed SQL command retrieves data about call dated in the table at the beginning of the investigation (Figure 79.). Epoch 1512211049405 is 2.12.2017 11:37:29.405.

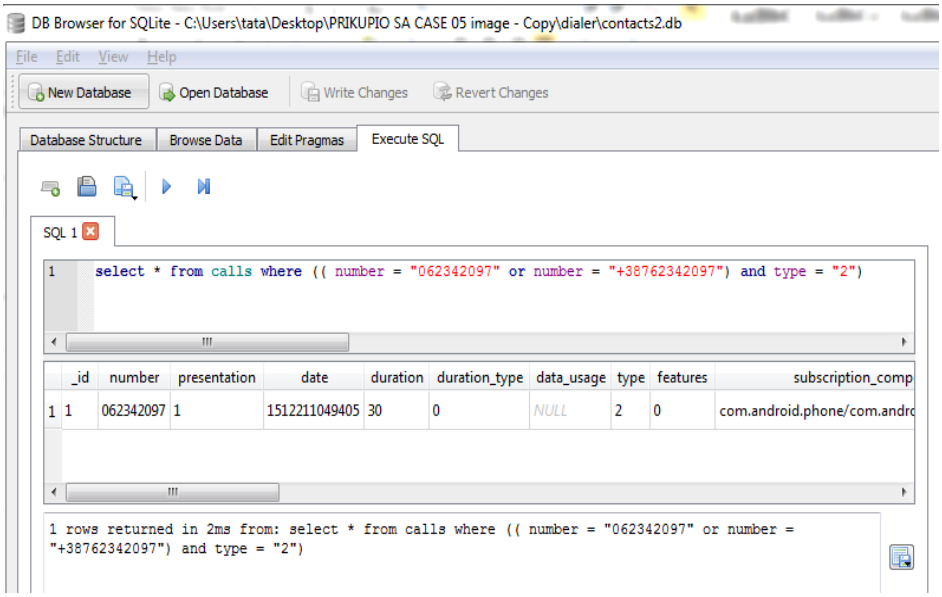


Figure 79. Retrieve Data About Calls from Table Calls

Coco Message Investigation

Coco messenger is not a widespread application. It supports messaging and voice communication. According to the previous analysis and application location mapping database, 59317329_coco.db is located in /data/com.instanza.cocovoice/databases. Initial data we were searching for is shown in Table 10.

TABLE 10. Coco Message Investigation

Report 062342097	Content	Date/time of receipt
Coco message	Careful with your door lock	3.2.2018 15:25
Coco message	You promised me not to leave me alone. Now you will regret.	2.2.2018 10:42

The structure of database after the extraction to the operational folder is shown in Figure 80.

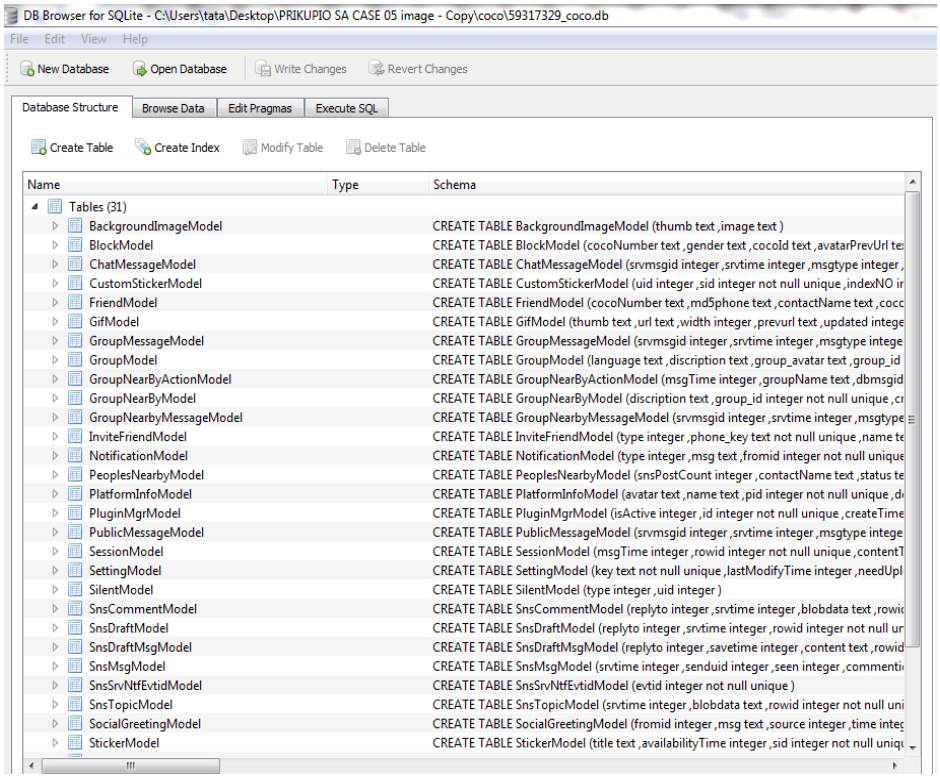


Figure 80. 59317329_coco Database Structure

Searching for the message "Careful with your door lock".

Table ChatMessageModels should have data related to messages. Executed SQL command did not have any data about the message (Figure 81).

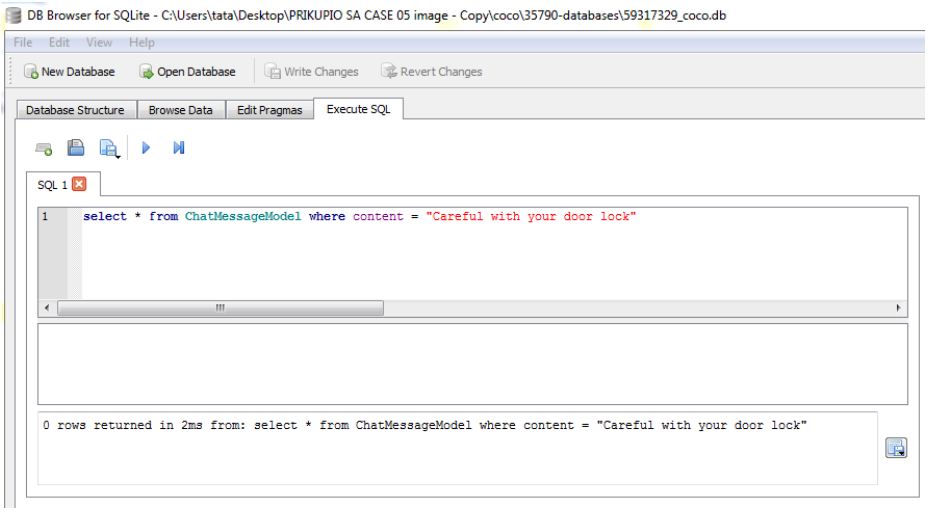


Figure 81. Retrieve Data about Chat Message from Table Content

SQLite-Deleted-Records-Parser tool retrieved deleted database data from the source file database 59317329_coco.db and output file coco.txt. After that, the execution message was found (Figure 82).

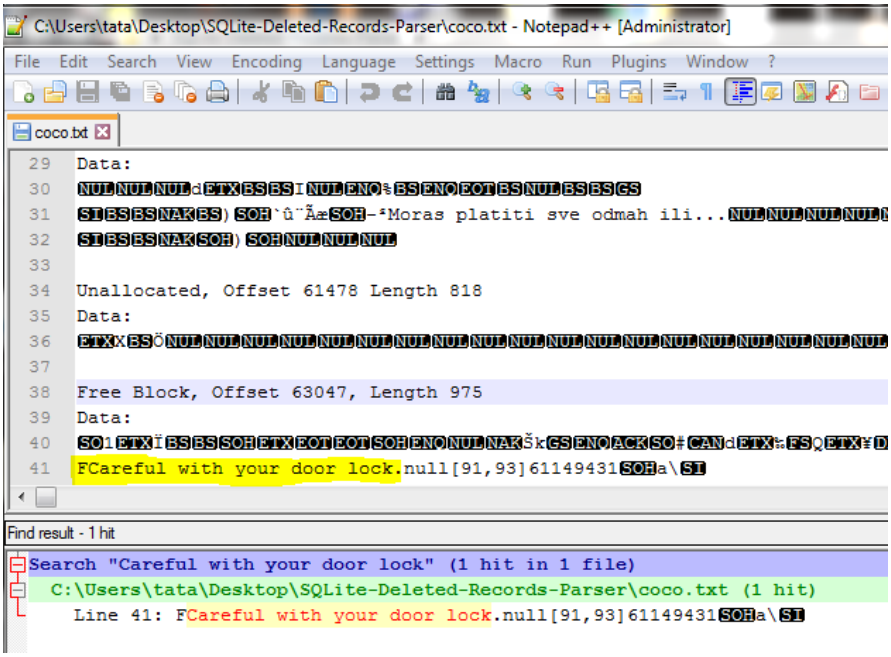


Figure 82. Recovered Evidence Message from Deleted Database Record

Searching for the Message "You promised me not to leave me alone. Now you will regret."

Table ChatMessageModels should have data related to messages. Executed SQL command retrieved data about the call dated in the table at the beginning of the investigation (Figure 83). Epoch 1517564524520 is 2.2.2018 10:42:04.520.

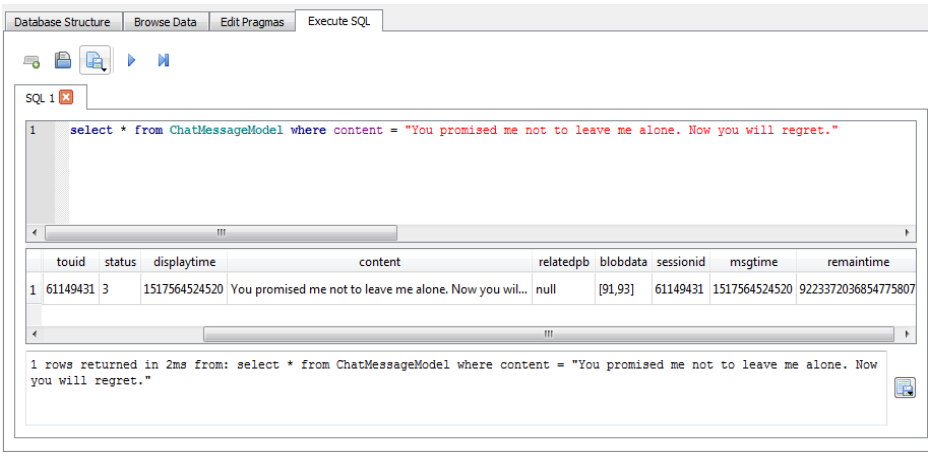


Figure 83. Retrieve Data about the Message from Table Content

Investigation Findings

The investigation was completed by summarizing discovered digital artefacts on the perpetrator's Android mobile device. Quantitative data is shown in Table 11.

TABLE 11. Quantitative Data about Found Evidence

	Number of reported/expected digital artefacts	Logically acquired artefacts	Physically acquired artefacts
Viber	3	0	3
SMS	1	0	1
Coco	2	0	2
GSM calls	1	1	1
Total	7	1	7
Percentage	100%	14.2%	100%

Summary of data shows that the team proved the existence of the searched data in the mobile device. Investigation started with 7 reported messages/calls/photos. That was the foundation for defining the scope of the investigation and tools needed to carry it out. During processes, two methods of data acquisition were used, namely Logical and Physical data acquisition. It is obvious that using AF Logical OSE tool for the logical acquisition was not enough to obtain the necessary data – especially when data was deleted (SMS) – and other Internet services such as Viber and Coco messenger and deleted photographs.

Ending Investigations

All collected evidence findings were submitted according to the rules and procedures. The report is handed over to the authorities together with the evidence. The evidence was used in the court. It is not known what happened to the perpetrator.

Figure 84. shows the report summary with data about case such as case name, case number, examiner name, time zone, and the location of the taken image.

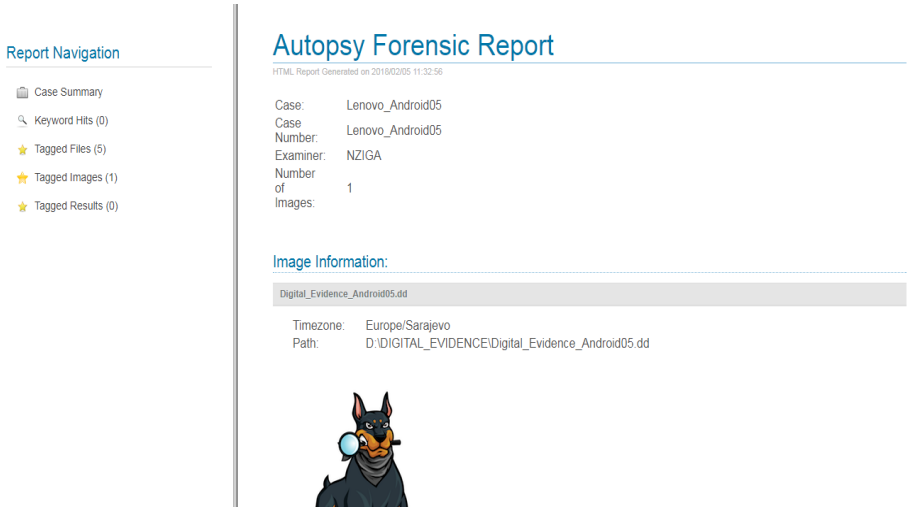


Figure 84. Report Summary

Figure 85. shows tagged files for evidence. Evidence list contains the exact location of evidence within the partition.

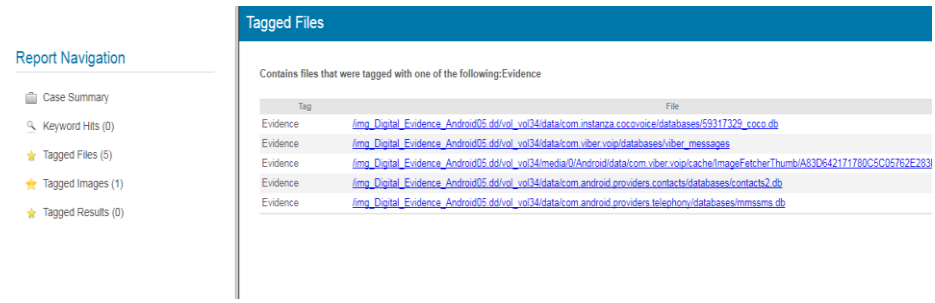


Figure 85. Report of the Evidence Tagged Files and Locations

Report navigation offers grouping of data by categories of keywords hits, tagged files, tagged images, and tagged results. The report showed in Figure 85. included files and images as the evidence trail.

Case 3: Database forensics – user complaints on high bills

The complain centre in the Internet provider's company received the complaint from the customer about high bills at the end of the month. Management ordered forensic analysis, so internal forensic investigators began the forensic analysis on the RACUNI_USER_USER table where customer account details were kept to investigate the potential suspicious activity. The forensic analysis of the table RACUNI_USER_USER should indicate if there was an unauthorized change, and if yes, when and who did the changes.

The report with IBM Guardian was created for the given table, and the result of the report is shown in Figure 86.

Figure 86. IBM Guradium report for the customer complaints

The report shows details indicating that there has been a change in the table, that is, in the set values for MOBILE, FIXED for two customers and INTERNET for one customer. We can notice that DB USER is an unclassified person (attacker) who came from the IP address: aaa.bbb.cc.dd where the service account ESJEDNICE_TST was logged on.

By inspecting a HOST that corresponds to an IP address, it was confirmed that it is a file server of the Internet provider company (BH TELECOM) domain.

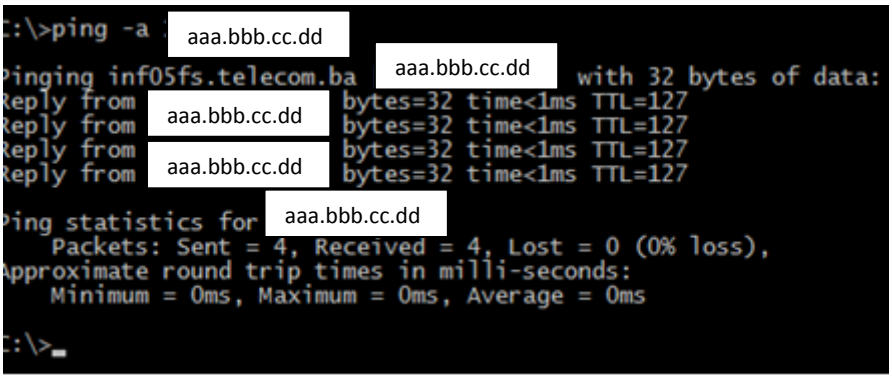


Figure 87. IP resolution

Digital forensic investigators detected a criminal attempted to conceal evidence by logging in with a service account on the FILE server. Attacker used the file server to start SQLPLUS tool with the user ATTACKER to access the database and make unauthorized changes in the table.

The next logical step in the forensic investigation was to try to find out who was hiding behind the username ATTACKER, or who gave the rights (rights to the database) to the ATTACKER who made the changes in the table. Information is presented in Figure 88.

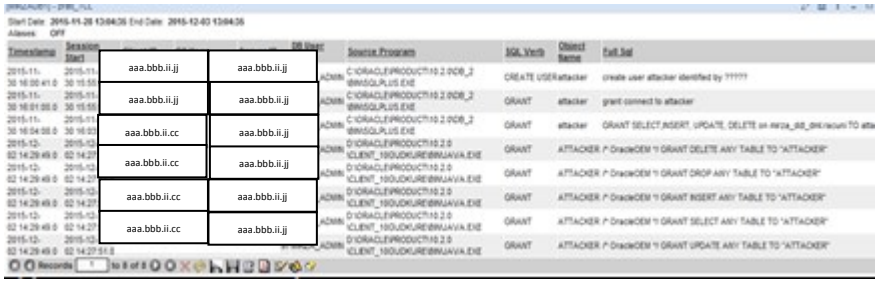


Figure 88. Report from IBM Guardium shows ATTACKER creator

User ATTACKER was created by one of the administrators (MIRZA_ADMIN) through SQLPLUS on a local server, and granted through the Oracle Enterprise Manager Tool.

Case 4: Database forensics – Salaries data leakage

Company management initiated the forensic analysis after salary details were revealed in the media. Due to disclosure of the confidential information, a written request from the management was made to conduct a detailed forensic investigation of the database to determine who and how accessed the table with data about salaries. Fact known by forensic investigators was that there were two tables containing the incriminated data. One table contained data on salaries and another on employee names. The next report in the IBM Guardium tool, which follows the sensitive tables, shows the events related to this case (Figure 89.).

Figure 89. IP address, username, and SQL command

The first report shows that the undefined user POM_2015 connected to the database using the SQLPLUS tool, from the machine whose IP address is: aaa.bbb.ee.ff where the user is esjednice_stst1, and created tables with contents of the table PLATE (SALARIES) and UPOSLENIC_FIRME (COMPANY_EMPLOYEES).

Figure 90. shows DNS name of PC with address aaa.bbb.ee.ff which determines PC *ucionica* (classrom1). This is an example of a fraudulent activity where the HOST classroom1 is used to hide database access traces. Another important issue is that the access to tables with salaries and table with names was not direct. Rather, in order to cover tracks, two so-called *"help tables"* were created (IZVJ_2015 and HR_IZVJ_2015) with data from sensitive tables.

Figure 90. IP Address name resolution

From the fact that two additional tables were created for sensitive data access, we can understand that the attacker assumed that there were certain tools which followed the access to the above tables, and tried to obtain data from sensitive tables indirectly. The next step for the forensic team was to go into a deeper analysis of user POM_2015 and tables created by this user which indicated illegal activities on the database.

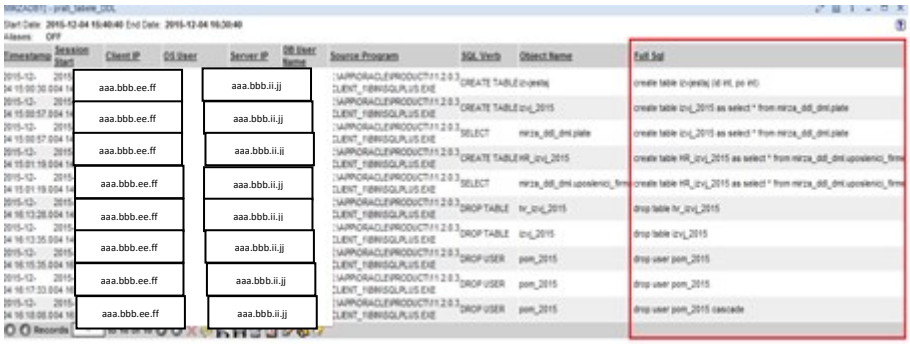


Figure 91. View detailed POM_2015 user-related activities

Figure 91. shows the chronological overview of the user POM_2015 and administrator MITZA_DBA criminal activities on the database. After POM_2015 created the auxiliary tables from which s/he collected the information, s/he wiped it out to cover up the evidences. However, the IBM Guardium tool recorded one more item here, which is that in this procedure, a user (in this case, MIRZA_DBA) appeared, which erased the user who committed the criminal activity.

Forensic analysis led to very important information indicating a valid trace, i.e., the fact that the administrator (MIRZA_DBA) was actually responsible for the criminal activity (Figure 92.).

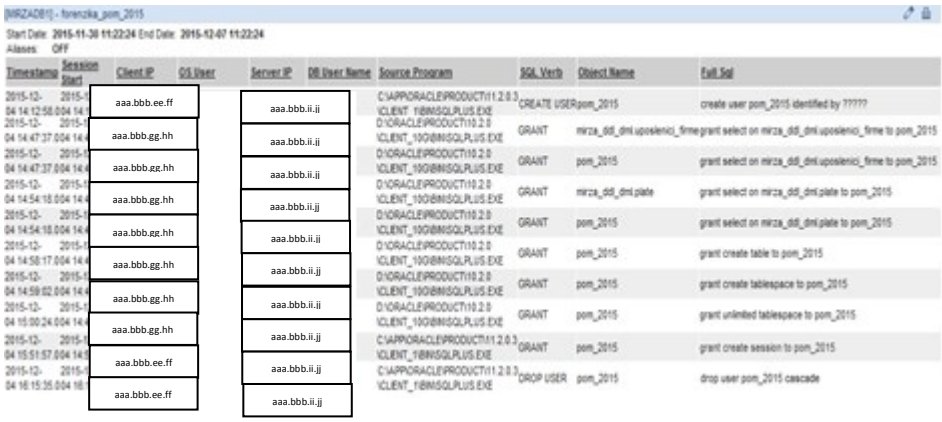


Figure 92. Details of the report about the creation of the user POM_2015 and granted access rights

The forensic analysis presented in the previous report clearly shows when the user was created and in what way, and how he obtained privileges over the tables in order to access the database. In conclusion, we can notice that

the account and tables were deleted in order to try to conceal the proof of the criminal activity.

Case 5: Database forensics – data deletion

Company's marketing department discovered that data from a database was deleted and requested the investigation. Human resources also discovered that the column with monthly employees' salaries in the database table was deleted. Thus, they initiated data recovery from the backup, however, before the procedure of restoring data from the backup, management wanted to report who, what, when, and in what way deleted data from the database.

The report generated using IBM Guardium for the table where the data was deleted shows who deleted data, when and how that happened, and which tool was used.

Figure 93. A forensic report related to deleted data in the table

As shown in the IBM Guardium report, the user who is responsible for deleting all data from the table NOVE_USLUGE is TRON555.

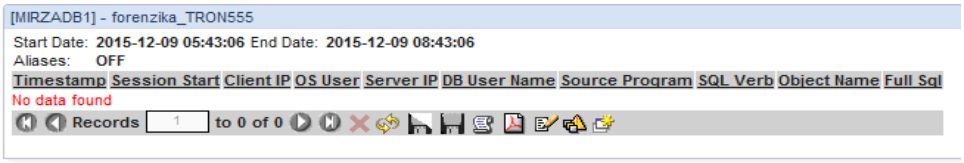


Figure 94. Report on details of creation and assignment of privileges for the user TRON555

However, when the team tried to further explore the origin of the user, i.e. when it was created and who created it in the IBM Guardium, they failed.

The forensic investigator realized that the attacker was well-acquainted with the IBM Guardium system and managed to hide the trace of creating and granting rights to the user who cleared all data in the table.

The following forensic analysis showed that the attacker knew that there were users which were not recorded by the IBM Guardium when monitoring changes in the database. These users began the service and they were used to run backup scripts, which were excluded from monitoring through the IBM Guardium tool which was permitted by the management.

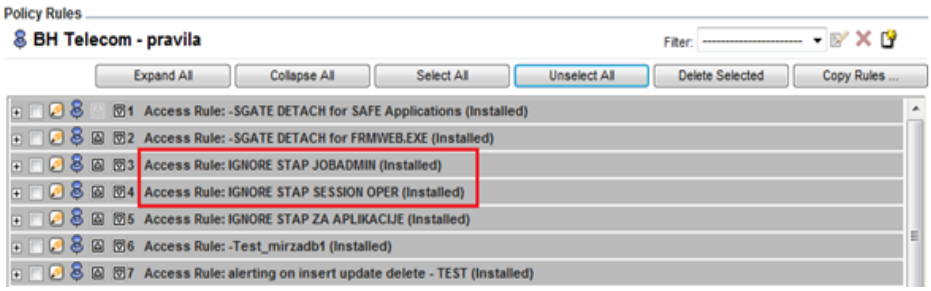


Figure 95. View exception rules for users who are not treated through IBM Guardium

Figure 96. shows that the attacker might have used one of the two mentioned users in order to circumvent the system and thereby attempt to hide the true trail indicating who is responsible for an unauthorized action of deleting data in the table. However, s/he did not consider that the forensic investigator had other methods and tools which could lead to

evidence. By inspecting the redo log file with the LogMiner tool, the requested response indicated which user was behind the user TRON555.

Data Grid

Data Grid | select timestamp,username, SQL_redo from v$logmnr_contents where sql_redo like '%tron555%'

TIMESTAMP	USERNAME	SQL_REDO
7.12.2015 15:50:12	OPER	create user tron555 identified by VALUES 'B86A0F94C1762433' ;
7.12.2015 16:00:46	OPER	grant delete on mirza_ddl_dml.nove_usluge to tron555;
7.12.2015 16:07:05	OPER	grant create session to tron555;
7.12.2015 16:11:15	OPER	grant delete on mirza_ddl_dml.test_nove to tron555;
7.12.2015 16:14:55	OPER	grant drop any table to tron555;

Figure 96. LogMiner Detailed report for the creation and permitting access for the TRON555 user

However, since this was the service user account, the forensic investigator had to investigate further to see who enabled the user OPER to create and assign rights to users in the database or delete data from the table. The report received through the IBM Guardium gave the answer to this question and at the same time the solution to another request that came from the Human resources regarding deleted data containing salaries from the NAKNADE_USER table.

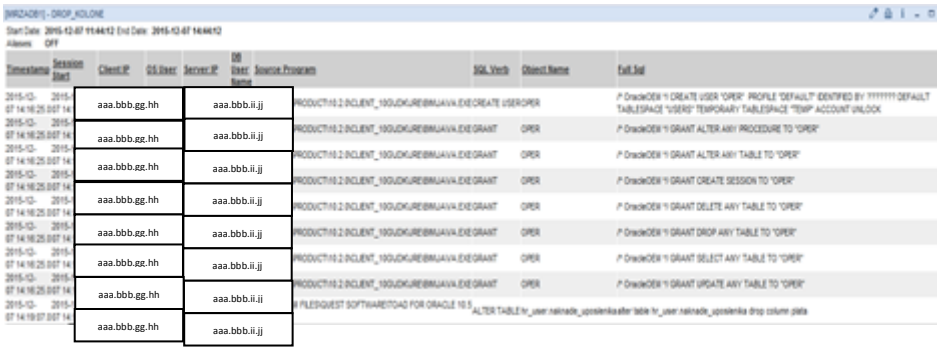


Figure 97. Details of the report related to deleting a column in the table

The report shows that the user OPER was created on the computer whose IP address was aaa.bbb.gg.hh and on which the user MIRZAHAL has been registered with the help of the SYS base user. The user OPER was assigned rights to delete the column in the table.

The report from logMiner shows that the same user (OPER) was used to create another user (TRON555) who deleted the data from the NOVE_USLUGE table.

This test scenario is an indication that an attacker will always search for a "weak point" of the systems, programs, equipment, or devices. Attackers seek weak points in an attempt to hide themselves, thus avoiding any possible liability for the committed crime.

Summary

Cyber security is a subset of the information security which deals with the security of information stored in digital form and transferred over communication links. A great part of information security related standards deals with cyber security issues. Almost daily, media reports reveal cyber security related incidents. After the historical analysis, we can conclude that we will see an increase in incidents of this type, especially as more services and users use digital technology in their everyday work and life.

Knowledge acquired

Forensic data recovery of files on PC, forensic data recovery of Viber, voice call, SMS, and Coco on an Android mobile phone. Database

forensic related to user complaints on high bills, salaries data leakage, and data deletion.

Review questions

1. How attacker can hide wrongdoings?
2. Location of database on mobile Android phone?

Further readings

- Digital transformation: online guide to digital business transformation https://www.i-scoop.eu/digital-transformation/
- The Cyber Security Management System: A Conceptual Mapping, SANS Institute InfoSec Reading Room https://www.sans.org/reading-room/whitepapers/basics/cyber-security-management-system-conceptual-mapping-591

Video resources

- The case of the stolen exams

https://www.youtube.com/watch?v=1BVG6cmPlPk

- Digital Forensics – Famous Cases

https://www.youtube.com/watch?v=gPuugbpLOeI

6. Conclusions

Chapter abstract

Chapter goals: To summarise book goals and review gained knowledge.

Cybercrime is much different from the conventional crime related to the physical world. There are a lot of challenges for the law enforcement and organisations who are victims of the cyber-crime. There is not much difference between crimes in cyber and physical space, however, in cyber space there is a lot more data and ways in which criminals could hide it. Also, it is more challenging to perform the digital forensic investigation because specific data can be found in volatile or non/volatile memory. Another challenge is the fact that criminals do not have boundaries, while boundaries between different countries' jurisdictions exist.

Digital forensics is still in the process of development, and is constantly being upgraded with the latest scientific advancements and new practices. Technology progress must be followed by the goal to be ready to face new challenges in form of crime techniques in the cyberspace.

Additional professional, legal, and scientific efforts have to be invested to improve the existing practices to combat cyber criminals. It is a professional duty to support activities and develop techniques and infrastructures to fight against the misuse of cyber resources.

This book presents the range of free digital forensic tools which can be used by students as a guide to develop and practice their skills.

We presented several simulated cases of digital forensic investigations with documented evidence, and steps which can be followed in similar situations.

Furthermore, expert witnesses can present the evidence from real digital forensic cases at the court by following steps and using tools presented in this book, or similar procedures and tools accepted in local and international jurisdiction.

Finally, the digital forensic investigator must continuously upgrade knowledge about cases, tools, best practices, and technology. Technology is developing very fast, so even some tools presented in this book might already be outdated, which is why reading and lifelong learning is important for a successful combat against the cyber-crime.

Appendix – Consent Form

I, _____(name and surname), (DOB ____/____/____), hereby authorizes _____ _____, an _____ (function title), to take custody and analyse the items detailed below for evidence. I understand that copies of the contents of the items, including all files and data, may be copied and retained for the analysis. I also understand that the analysis of the copies of the media may continue even after the items designated for the analysis are returned. I provide my consent to this analysis freely, willingly, and voluntarily, and with the knowledge that I have the right to refuse to consent. I provide my consent without fear, threat, coercion, or promise of any kind.

Device	Serial number	Additional owner/user details

Owner's printed name	Signature
Witness' printed name	Signature
Witness' printed name	Signature

Appendix – Incident response form

General data about incident

- System under attack
- Incident investigation in progress
- Incident closed

Required assistance:_____

Which data, service, project is under an impact:

_____

_____

Type of incident

- Malicious software
- DoS/DDoS attacks
- Unauthorized access
- Leakage of data and information in public

Date and time of the incident:

_____

Brief summary:

_____

_____

_____

Details for malicious software:

Source (mail, web page, mobile memory such as USB):

_____

Type: (virus, Trojan, worm, spyware, other):

_____

_____

DoS / DDoS attack

Attack source:

_____

Service attacked (OS version, IP address):

_____

Type of DoS / DDoS traffic:

_____

Details for an unauthorized access:

_____

_____

Leakage of data and information in public:

Appendix – Digital forensic process

List of Figures

List of Tables

Acronyms

ACK Acknowledgement

CERT Centre for Emergency Report Team

CISA Certified Information Security Auditor

CISM Information Security Manager

CISP Certified Information Security Professional

CISO Chief Information Security Officer

CISWG Corporate Information Security Workgroup

CSO Chief Security Officer

DMZ Demilitarised zone

DoS Denial of Service

DDoS Distributed Denial of Service

DML Data Manipulation Language

FTP File Transfer Protocol

HTTP Hyper Text Transfer Protocol

IA Internal Auditor

ICMP Internet Control Message Protocol

IDS Intrusion Detection System

IP Internet Protocol

IPS Intrusion Prevention System

IEC International Electrotechnical Commission

IEEE Institute of Electrical and Electronic Engineers

IPX Internetwork Packet Exchange

ISACA Information Systems Audit and Control Association

ISM Information Security Manager

ISMS Information Security Management System

ISO International Standardisation Organisation

ISSEA International Systems Security Engineering Association

IT Information Technology

KPI Key Performance Indicator

LAN Local Area Network

MIB Management Information Base

NIST National Institute of Standards & Technology

NMS Network Management Station

OID Object identifier

OSI Open System for Interconnection

PDCA Plan Do Check Act

QoS Quality of Service

SMTP Simple Mail Transfer Protocol

SNMP Simple Network Management Protocol

SQL Simple query language

SYN Synchronize

TCP Transmission Control Protocol

UDP User Datagram Protocol

UPS Uninterruptable Power Supplies

VPN Virtual Private Network

WAN Wide Area Network

References

AccessData. (2006). White paper: MD5 collision – The effect on Computer Forensics. Available from: https://ad-pdf.s3.amazonaws.com/papers/wp.MD5_Collisions.en_us.pdf

Afonin, O. & Gubanov, Y. (2013, May 28). Catching the Ghost: How to Discover Ephemeral Evidence through Live RAM Analysis. *Forensic magazine*. Available from: http://www.forensicmag.com/article/2013/05/catching-ghost-how-discover-ephemeral-evidence-through-live-ram-analysis

Appazov, A. (2014). *Legal Aspects of Cybersecurity*. Faculty of Law University of Copenhagen. Retrieve from: http://justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningspuljen/Legal_Aspects_of_Cybersecurity.pdf

Android. (2017), Application Security, Available from https://source.android.com/security/overview/app-security accessed 25.9.2017

Android. (2017), *Platform Architecture*, Available from https://developer.android.com/guide/platform/index.html#art accessed 23.12.2017

Ayers, R. Brothers, S and Jansen, W. (2014), *Guidelines on Mobile Device Forensics*, NIST Special Publication 800-101: Available from http://dx.doi.org/10.6028/NIST.SP.800-101r1, 20.12.2017 [Accessed on 12.01.2019]

Banking and Insurance, 2017 Available from: http://en.finance.sia-partners.com/20171211/cyber-incident-response-how-strong-your-incident-response-plan, [Accessed on 20.01.2019]

Boccaccini, M.T. (2002). What Do We Really Know about Witness Preparation? *Behav. Sci. Law 20: 161–189*. DOI: 10.1002/bsl.472

Burnette, Michael W. "Forensic Examination of a RIM (BlackBerry) Wireless Device." June 2002. Available from: http://www.rh-law.com/ediscovery/Blackberry.pdf (accessed 11.1. 2018)

Catts E.P. & Goff M.L. (1992). *Forensic entomology in criminal investigations*. Annu Rev Entomol. Vol.37:253-272. DOI: 10.1146/annurev.en.37.010192.001345

Carrier, B. and Spafford, E. (2004). An Event-Based Digital Forensic Investigation Framework, *The Digital Forensic Research Conference*, p2-3. Available from: https://www.dfrws.org/sites/default/files/session-files/paper-an_event-based_digital_forensic_investigation_framework.pdf [Accessed on 20.01.2019]

Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers*

and the Internet (3rd ed.). Elsevier Inc. Available from: http://booksite.elsevier.com/samplechapters/9780123742681/Front_Matter.pdf 309 [Accessed on 11.02.2019]

Cellebrite (2017), *Cellebrite's Universal Forensic Extraction Device (UFED)*, Available from https://www.cellebrite.com/en/home/ (accessed 21.1.2018)

Cosic, J., Cosic, Z., & Baca, M. (2011). An ontological approach to study and manage digital chain of custody of digital Evidence, *Journal of Information and Organizational Sciences, 35* (1): 1-13

Chow, K.P. & Shenoi S. (2010, January), *Advances in Digital Forensics VI*. Sixth IFIP WG 11.9 International Conference on Digital Forensics.

Cho, W. K. T., & Gaines, B. J. (2007). *Breaking the (Benford) Law: Statistical Fraud Detection in Campaign Finance*. The American Statistician, 61(3), 218-223.

Criminal Justice Degree Schools (2019), Available at: https://www.criminaljusticedegreeschools.com/criminal-justice-degrees/computer-forensic-degree/ [Accessed on 20.02.2019]

Crime Museum, 2019 Edmond Locard, Available at: https://www.crimemuseum.org/crime-library/forensic-investigation/edmond-locard/ [Accessed on 20.02.2019]

Data, Merriam-Webster 2019 Available at: https://www.merriam-webster.com/dictionary/data [Accessed on 02.07.2019]

Desertcart. (2018), *Palm V Hand held PDA,* Available from https://www.desertcart.ae/products/15557437-palm-v-hand-held-pda htm [Accessed on 20.01.2019]

Diekmann, A. (2012), Making Use of "Benford's Law" for the Randomized Response Technique, Article in Sociological Methods & Research, DOI: 10.1177/0049124112452525 Available from https://www.researchgate.net/profile/Andreas_Diekmann2/publication/269815391_Making_Use_of_Benford%27s_Law_for_the_Randomized_Response_Technique/links/553bae070cf245bdd766705f.pdf [Accessed on 20.01.2019]

(DFRWS, 2001), A Road Map for Digital Forensic Research Available from: http://dfrws.org/sites/default/files/session-files/a_road_map_for_digital_forensic_research.pdf [Accessed on 02.02.2019]

Edson, J. (2011, July 25). *A Brief History of Forensic Science.* Australia's Science Channel. Available from: http://riaus.org.au/articles/a-brief-history-of-forensic-science/ [Accessed on 20.12.2018]

Forensic, Merriam Webster, 2018, Available at: https://www.merriam-webster.com/dictionary/forensic, [Accessed on 20.12.2018]

Forensics and Benford's Law. (2018), *Event Log Explorer*, https://eventlogxp.com/blog/forensics-and-benfords-law/ accessed 20.1.2018

Gadgeter (2018), *RIM BlackBerry 950 Review*, Available from https://the-gadgeteer.com/2001/02/26/rim_blackberry_950_review/ accessed 10.1.2018

Google, 2018, Etymology of word Forensic, Available at: https://www.google.ba/search?rlz=1C1AVNC_enBA595BA595&q=forensic+etymology&spell=1&sa=X&ved=0ahUKEwi9offs6qPeAhVECywKHaDMCM8QBQgnKAA&biw=1366&bih=657 [Accessed on 26.10.2018]

Grand, J. (2002) pdd: Memory Imaging and Forensic Analysis of Palm OS Devices, https://www.researchgate.net/publication/2490864_pdd_Memory_Imaging_and_Forensic_Analysis_of_Palm_OS_Devices (accessed 20.1.2018)

History of Fingerprints, (2018) Crime Scene Forensic, LLC, Available at: http://www.crimescene-forensic.com/History_of_Fingerprints.html [Accessed on 01.11.2018]

IBM Guardium, (2019) IBM Guardium Data Protection for Databases, Available at: https://www.ibm.com/us-en/marketplace/ibm-guardium-data-protection [Accessed on 01.11.2018]

IBM Knowledge Center, 2013 How a Q Capture program works with the Oracle LogMiner utilit, Available at: https://www.ibm.com/support/knowledgecenter/SSTRGZ_10.2.0/com.ibm.swg.im.iis.repl.qrepl.doc/topics/iiyrqcapclogminercnc_ep.html [Accessed on 15.11.2018]

IDC. (2017), *Smartphone OS Market Share*, 2017 Q1, Available at: https://www.idc.com/promo/smartphone-market-share/os accessed 5.12.2017

IIA, 2019, Institute of Internal Auditors, 2019, Definition of Internal Auditing, 2019, Available at: https://na.theiia.org/standards-guidance/mandatory-guidance/pages/definition-of-internal-auditing.aspx [Accessed on 20.01.2019]

IOCE. (1999). IOCE Principe & Definitions.
Available from: https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm [Accessed on 20.01.2019]

Information, Merriam-Webster 2019, Available from: https://www.merriam-webster.com/dictionary/information [Accessed on 20.05.2019]

Information system, Britanica, 2019, Information system, an integrated set of components for collecting, storing, and processing data and for providing information, knowledge, and digital products, 2019 Available from: https://www.britannica.com/topic/information-system [Accessed on 20.01.2019]

Information technology, Merriam-Webster, 2018, Available from: https://www.merriam-

webster.com/dictionary/information%20technology, [Accessed on 20.01.2018]

Infosec Institute. (2017), *Computer Forensics Salary Data*, http://resources.infosecinstitute.com/category/computerforensics/introduction/computer-forensics-salary-data/#gref accessed 19.12.2017

Kaur, R. & Kaur, A. (2012). Digital Forensics. *International Journal of Computer Application (0975-8887), 50*(5), 2-4. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.258.7882&rep=rep1&type=pdf [Accessed on 20.01.2019]

International Telecommunication Union. (2014). *Understanding cybercrime: phenomena, challenges and legal response*. Report. Available from: http://www.itu.int/en/ITU-D/Cybersecurity/Documents/cybercrime2014.pdf [Accessed on 20.01.2019]

Kremic E.; Subasi A.; Hajdarevic K., Face recognition implementation for client server mobile application using PCA, Proceedings of the ITI 2012 34th International Conference on Information Technology Interfaces, Year: 2012 Page s: 435 – 440

Law Enforcement Cyber Center (2017), Available at: http://www.iacpcybercenter.org/officers/digital-evidence/ accessed 15.12.2017

Lee, K. Lee, Y. Lee, H. and Yim, K. (2016), *A Brief Review on JTAG Security*, 2016 10th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing DOI 10.1109/IMIS.2016.102

Levin. J, (2015), Android Internals: Power User's View (1st edition), Cambridge: Technologeeks.com

Litchfield D., Oracle Forensic Part 1: Dissecting the Redo Logs, An NGSSoftware Insight Security Research (NISR) Publication ©2007 Next Generation Security Software Ltd.

Logilink,2019, Available at: http://www.logilink.eu/media/images/produkt/_800/CR0012.png [Accessed on 20.11.2018]

Lynch, V.A. & Duval J.B. (2011). Forensic Nursing Science (2nd ed.). Elsevier Mosby p2

Marcella A. J. and Menendez D. Cyber Forensic, Second Edition, Auerbach Publication, 2008

Massachusetts Digital Evidence Consortium, 2015, Digital Evidence Guide for First Responders,
Available from: http://www.iacpcybercenter.org/wp-content/uploads/2015/04/digitalevidence-booklet-051215.pdf [Accessed on 20.11.2018]

Nanda A., 2019 Transaction Management with LogMiner and Flashback Data Archive, Available from: http://www.oracle.com/us/solutions/11g-transactionmanagement-092065.html [Accessed on 20.11.2018]

Nanda A. and Burleson D.K., Oracle Privacy Security Auditing, Rampant Techpress, 2003

National Institute of Justice. (2004). *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*. Available from: https://www.ncjrs.gov/pdffiles1/nij/199408.pdf

Nelson, B., Phillips A., & Steuart C. (2015). *Guide to Computer Forensics and Investigations* (5th ed.). Course Technology. Available from: https://books.google.ba/books?id=PUh9AwAAQBAJ&pg=PA137&dq=what+is+digital+evidence+SWGDE&hl=en&sa=X&ved=0ahUKEwii87LhrqnRAhUCVhQKHTsIAb4Q6AEIMTAB#v=onepage&q&f=false

NIST. (2004). *Digital Data Acquisition Tool Specification, Public Review of Version 4.0*. Available from: http://www.cftt.nist.gov/Pub-Draft-1-DDA-Require.pdf

NIKSUN NetDetector, 2018 Available at: https://www.phoenixdatacom.com/product/niksun-netdetector-packet-capture-network-security-forensics/ [Accessed on 20.12.2018]

Open University, 2018, Different types of digital forensic, Available at: https://www.open.edu/openlearn/science-maths-technology/digital-forensic/content-section-4.3, [Accessed on 20.12.2018]

(Oracle, pp. 79) Database Administrator's Guide, Available at: https://docs.oracle.com/cd/B28359_01/server.111/b28310/onlineredo001.htm#ADMIN11302 [Accessed on 15.02.2019]

Oracle Fine Grained Auditing, Available at: https://www.oracle.com/technetwork/database/security/index-083815.html2019 [Accessed on 18.02.2019]

Oracle DBA_FGA_AUDIT_TRAIL Available at: https://docs.oracle.com/cd/B19306_01/server.102/b14237/statviews_3115.htm#REFRN23075 [Accessed on 18.02.2019]

Oracle LogMiner, 2019, Available at: https://www.oracle.com/technetwork/database/features/availability/logmineroverview-088844.html, [Accessed on 25.03.2019]

Pollit, M. (2017, January 15). *A history of digital forensics*. Available from: https://pdfs.semanticscholar.org/0d15/132439fc1de82724dd06effff5a782eefeac.pdf

Recombu. (2017), *Android updates*, Available from https://recombu.com/mobile/article/what-is-android-and-what-is-an-android-phone_M12615.html , accessed 25.09.2017

Renkforce, 2019 Available at: https://www.conrad.com/p/renkforce-rf-docking-06-usb-30-esata-sata-4-ports-hdd-docking-station-1305502 [Accessed on, 14.03.2019]

Road MASSter 2, 2019 Available at: http://dfrt.blogspot.com/2007/01/forensic-tools-hardware.html [Accessed on, 01.03.2019]

Roy, NR. Khanna, AK. Aneja, L (2016), *Android Phone Forensic: Tools and Techniques* International Conference on Computing, Communication and Automation (ICCCA2016) Available from http://ieeexplore.ieee.org/document/7813792/

Ryder, K. (2002). Computer Forensics – We've Had an Incident, Who Do We Get to Investigate? *SANS Institute InfoSec Reading Room*. Available from: https://www.sans.org/reading-room/whitepapers/incident/computer-forensics-weve-incident-investigate-652

ShareTechnote. (2017), Android ADB, Available from http://www.sharetechnote.com/html/Android/Android_ADB.html accessed 25.9.2017

Sapir, G.I. (2007, January 2). Qualifying the Expert Witness: A Practical Voir Dire. *Forensic magazine*. Available from: http://www.forensicmag.com/article/2007/01/qualifying-expert-witness-practical-voir-dire

Singh, N and, Bansal, R. (2015*), Analysis of Benford's Law in Digital Image Forensics*, Signal Processing and Communication (ICSC), 2015 International Conference

Sophos. (2018), *2018 Malware Forecast: ransomware hits hard, continues to evolve*, Available from https://news.sophos.com/en-us/2017/11/02/2018-malware-forecast-ransomware-hits-hard-crosses-platforms/ accessed 6.1.2018

Smith, W. (1867). *Dictionary of Greek and Roman Biography and Mythology Vol 1*. Boston: Little Brown and Company p209

SNOW, 2019, The SNOW Home Page, Available at: http://www.darkside.com.au/snow/ [Accessed on, 14.03.2019]

Startribune. (2018), *Minnesota detectives crack the case with digital forensics*, Available from http://www.startribune.com/when-teens-went-missing-digital-forensics-cracked-case/278132541/ accessed 10.1.2018

SWGDE, (2013) Best Practices for Computer Forensic, Scientific Working Group on Digital Evidence, Version: 3.0 (September 14, 2013) Available at: https://www.swgde.org/documents/Archived%20Documents/SWGDE%20Best%20Practices%20for%20Computer%20Forensic%20v3-0, [Accessed on, 29.10.2018]

UNODC. (2013). *Comprehensive Study on Cybercrime*. Available from: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

UNODC. (2013). Comprehensive Study on Cybercrime. (V.13-80699) Vienna: United nations office on drugs and crime

UN. (2000). *Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders.* (A/CONF.187/10). Available from: https://www.asc41.com/UN_Congress/10th%20UN%20Congress%20on%20the%20Prevention%20of%20Crime/013%20ACONF.187.10%20Crimes%20Related%20to%20Computer%20Networks.pdf

Vandeven, S. (2014). Forensic Images: For Your Viewing Pleasure. *SANS Institute InfoSec Reading Room.* Available from: https://www.sans.org/reading-room/whitepapers/forensics/forensic-images-viewing-pleasure-35447 [Accessed on, 15.01.2019]

Xplico (2019) Available at: http://www.xplico.org/wp-content/uploads/2008/11/xwi_email.png [Accessed on, 29.01.2019]

Whitecomb, C.M. (2002). An Historical Perspective of Digital Evidence: A Forensic Scientist's View. *International Journal of Digital Evidence 1*(1),1-3

Watson, D.A., Jones, A. (2013). Digital Forensics Processing and Procedures: Meeting the Requirements of ISO 17020, ISO 17025, ISO 27001 and Best Practice Requirements (1st ed.). London: Elsevier / Syngress.

Wiley Carol, What Is the Difference Between Computer Forensic & Digital Forensic? Available at: https://careertrend.com/facts-6733855-

difference-computer-forensic-digital-forensic-.html [Accessed on, 29.01.2019]

Williams A., Leaving a trace: Forensic science through history, BBC, Available at: https://www.bbc.com/timelines/zcq2xnb#zgsg4wx, [Accessed on, 29.10.2018]

Witte de With, 2019 https://www.wdw.nl/en/participants/rodolphe_archibald_reiss [Accessed on, 29.10.2018]

Wright, Paul M. "Oracle forensic" Oracle security best practice, Rampant Techpress; May 2007.

Yeatts, T. (2001) *Forensics: Solving the Crime*, Available from: http://connection.ebscohost.com/c/articles/15721149/chapter-one-james-marsh-toxicology

Index

About authors

Kemal Hajdarevic *PhD,* received B.Sc. from the Faculty of Electrical Engineering, University of Sarajevo, Bosnia and Herzegovina, M.Sc. and PhD from Leeds Metropolitan University/Leeds Beckett University, Leeds, UK. He is currently working at the Central Bank of Bosnia and Herzegovina as a Senior Internal Auditor for information Security and IT projects, and he has a teaching position at the Faculty of Electrical Engineering, University of Sarajevo.

Nermin Ziga *MSc,* received MSc from International Burch University. Nermin is an employee of Raiffeisen Bank, were he works as an Information Security Officer within Raiffeisen Bank's Security Department.

Mirza Halilovic *MSc,* received MSc and BSc from the Faculty of Electrical Engineering, University of Sarajevo. Mirza is the Head of IT department for monitoring, security, and data protection at BH Telecom d.d. Sarajevo.

Dr. Hamid Jahankhani: *The area of "Digital Forensics" and its challenges, is clearly one of the key issues facing both the scientific community, industries and other users alike. Clearly understanding the digital forensics in a step by step format would help the practitioners in this fast paced technology development era. I welcome this new book on "Digital Forensics Essentials" which also aims to address some of the emerging issues.*

Looking at the table of content there are clearly a number of interesting areas of research and hence this book will undoubtedly help researchers and practitioners alike. To my opinion the scope and coverage of this book adequately represent a balanced review of the digital forensics subject. I feel the primary audience for this book would be Researchers, Practitioners, PhD and Postgraduate students.

I highly recommend this book.

Dr. Jasmin Azemovic: *We are facing turbulent events in cyberspace, and digital forensics is on of dominant research topics which is continuously being updated with the latest scientific advancements. Innovations in digital revolution are evident and this book will help to face new challenges in digital era with goal to fight against crime in the cyberspace and committed with, and against digital infrastructures.*

Dr. Colin Pattinson: *History has shown that, whenever a powerful new technology is developed, the desire to misuse that power soon follows. The field of computer network technology is no exception. Indeed IT misuse, whatever the underlying motivation, must be one of most frequent forms of unwanted activity there is.*

The ability to determine that an event has taken place, to learn from it and - hopefully - to prevent it occurring again is a prime motivation for a forensic analysis. Understanding of any losses have occurred, and building a legally sustainable case against the perpetrators requires even higher levels of information gathering and retention. It is therefore important that the skills and knowledge necessary to conduct such analysis are available to organisations when needed.

This book provides a grounding in the tools and techniques necessary to investigate a range of attacks, showing the importance of a structured, logical and methodical approach.

It is recommended for graduate students and those specialising in IT forensics.