DIGITAL FORENSICS INVESTIGATION

PRAVEK DHINA THIRUMURUGAN
F21FO DIGITAL FORENSICS
H00453819

Table of Contents

Introduction

The goal of the Digital Forensic Imaging and Analysis is to describe procedures in the acquisition and analysis of digital media. This technique is useful in investigation processes as the first step in the imaging procedure helps in ensuring that the copied data is the same as the original one to be analyzed by the investigators while at the same time ensuring the authenticity of the original data through check-sums and bit to bit copies. This procedure also assure that the evidence collected had not been tampered and can be produced in court. The ensuing process of forensic evaluation entails the employment of apparatus in the extraction, examination, and analysis of relevant information regarding the case. Basically, by following the general procedures and forensic techniques, the forensic examiner can come across valuable data that may contribute to the investigation.

2. Core Sections

2.1 Forensic Imaging Process

2.1.2 Tools Used

The digital forensic investigation employed two primary tools: Some of the best and common ones include FTK Imager and Autopsy. All these tools have different roles in the total process of forensic and support the detailed analysis of digital evidence.

2.1.3 FTK Imager

FTK Imager is an effective forensic imaging application with the mission to create duplicates of the digital storage media (Şentürk *et al.* 2020). This utility needs to produce bit-by-bit images and this is important in order to safeguard the interferometer's Fast Fourier Transform (FFT) data in a way that will be Are it looking for? admissible and authentic in a legal manner.

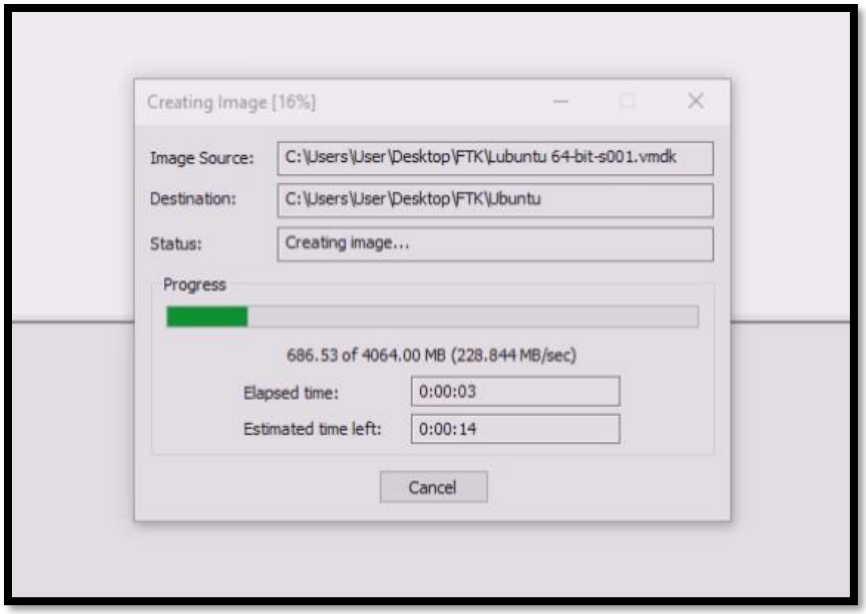

Figure 1: Creating the E01 file with FTK

(Source: Obtained from FTK Imager)

FTK Imager enables imaging of the hard drives, USB drives, or any other storage media that are part of a digital forensic investigation, The software supports creation of images in the E01 format, AFF and DD formats among others (Ozcan *et al.* 2021).

2.1.4 Autopsy

Autopsy is an open-source software which enhances the investigation of forensic images by providing an ideal environment to analyze it. Staying with the examiners' perspective, one should note that this tool allows it to perform various analytical operations, ranging from the analysis of the file system to the search for keywords and the construction of timelines.

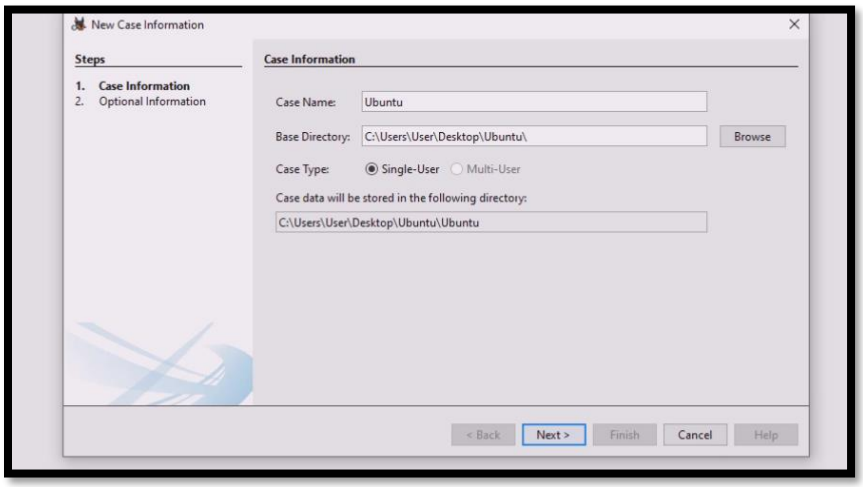

Figure 2: The Autopsy File Selection

(Source: Obtained from Autopsy)

The nature of the platform is that it enables organizing information related to an investigation into tags, preparing relevant reports, and other features. Thus, Autopsy can be used for simple straight-forward as well as complex cases and assists forensic analyst in finding relevant information and creating comprehensive report.

That is why, the usage of FTK Imager and Autopsy together guarantees a thorough examination of digital crimes. Although FTK Imager helps in acquiring an image of a suspect media and ensuring that data is not altered in its process, Autopsy helps in providing analysis on the images all acquired evidence goes through.

2.1.5 Steps Taken

In its creation, strict operations must be followed to guarantee the soundness of the forensic image of the seized digital device. It is as follows: Basic steps involved in the mastering of FTK Imager; Basic steps that are involved in Analytical process using Autopsy.

1. Preparation

There is a set of conditions that must be fulfilled prior to the beginning of the imaging process and the environment and tools required are listed below. This includes evaluation of the workplace for contamination, where the forensic workstation is configured, free of contaminants, and has FTK Imager and Autopsy installed.

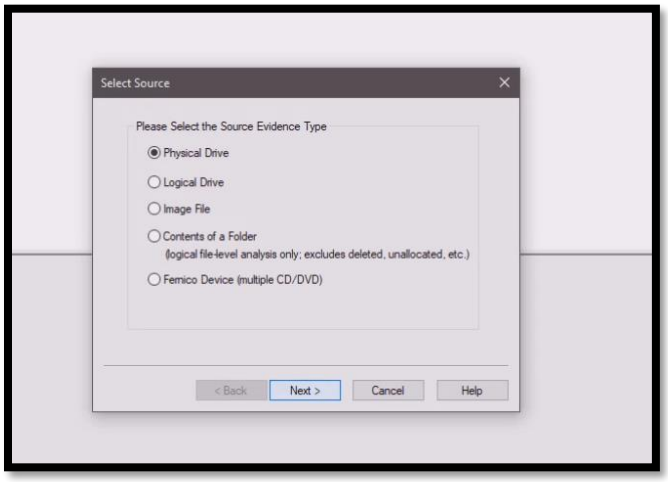

Figure 3: Preparation of FTK process

(Source: Obtained from FTK Imager)

For compact disc imaging, the storage media that is to be imaged has to be connected to the workstation on which this operation will be performed and preferably any documentation such as

chain of custody forms should also be prepared. The analysis of the hardware and the software environment allows for evaluating the functionality of all the elements and anticipating that no technical problem will occur during the long and complex process of imaging.

2. Creating the Forensic Image with FTK Imager

FTK Imager is employed in order to make a precise copy by means of the "Copy Disk" function of the digital storage device. The process starts by opening the FTK Imager and choosing the source storage media. The acquisition options in FTK Imager include the format commonly known as E01, AFF, or DD. Which format is used is dependent on the demands initiated by the investigation as well as the preferences concerning the treatment of evidence.

3. Verifying Image Integrity

After the preparation of the forensic image, confirmation and validation of the image are crucial to making sure that the copy is an original representation of the data. While imaging the disk, FTK Imager calculates hash values which are checked against the image file. These hash values are compared with the hash values of the original storage device to ensure no changes have been made.

4. Analyzing the Forensic Image with Autopsy

The forensic image acquired with FTK Imager is assessed with the help of the Autopsy tool. The analysis procedure starts with the importation of the forensic image in the Autopsy. The tool works on the scan of the image and creates an index of all the data present in the image in the form of File systems, directories and Actual files.

5. Documenting the Process and Chain of Custody

The last process that should not be overlooked in the course of the forensic imaging work is documentation. The documentations of all the activities that are carried out in the process of doing the imaging as well as the subsequent analysis are done to the finest detail. For example, status of the storage device at the beginning, imaging process, any generated hash values, and any complications observed.

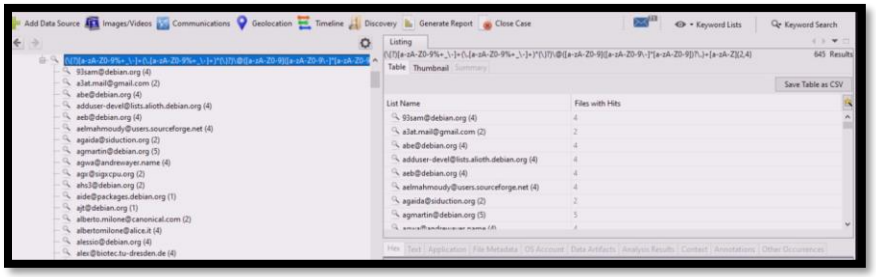

Figure 4: The Investigation in Autopsy

(Source: Obtained from Autopsy)

There is also documentation of the chain of custody, which shows all the persons who dealt with the piece of evidence, dates of transfers, and any alteration in the evidence's state. Documentation makes forensic easy to explain or defend in lawful proceedings and helps in review in case one wants to reverse the process in the future.

2.1.6 Chain of Custody

The components of the chain of custody are well important to preserve the quality of the evidence during the overall conducting of forensic investigation. It is an orderly filing of all legal papers from the onset of the investigation right up to the trial and beyond.

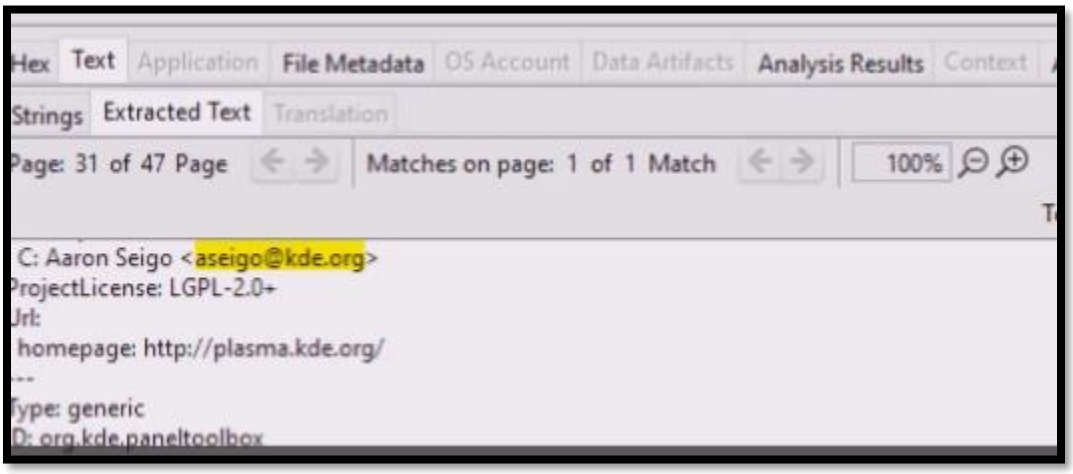

Figure 5: The Malicious mail in Autopsy

(Source: Obtained from Autopsy)

1. Documentation of Evidence Collection

The evidence collection process is to be documented and this marks the start of the chain of custody. These are the identification of the person who took the evidence, the date, time, and place of collecting the evidence, among others. All the damages to the evidence are recorded despite the preservation of the originals, and the type of evidence collected is also recorded. Proper documentation to this extent puts the jury in a position of easily linking the evidence to the personnel who handled it.

2. Handling and Transfer

Every time the evidence is touched or passed from one individual to the other, everything is well noted. Some of the rules include having the identity of persons with custody of the evidence, the date and time, and the reason of the transfer recorded. Each cash transfer's documentation is vital to establishing and preserving the record of the evidence, which helps avoid alteration or loss of critical data.

3. Storage Conditions

It is recorded that how the evidence should be stored to avoid any damages or spoilage takes place. Data is gathered regarding temperature, humidity, and other factors that define the storage conditions and the level of security. These records ensure that the evidence has been preserved under conditions that do not allow for its degradative or transformative conditions.

4. Evidence Access and Security

The collect accessible and controlled evidential data. The records of chain of custody relate on who has come into contact with the evidence and the reason of being near it. This helps to ensure that only the right people are touching the evidence which in turn helps to preserve the substance in question. To this effect, a virtually sequenced and tight chain of custody of the digital evidence must be sustained in order to show that the evidence is still genuine and has not changed along the process of digital forensics.

2.2 Forensic Analysis

2.2.1 Tools Used

FTK Imager

FTK Imager is the most commonly used forensic imaging tool characterized by its effectiveness in creation of an identical copy of the targeted digital media. It's designed to acquire a clone of the drives, without modifying any of the original data in the course of the forensic examination.

Autopsy

Autopsy is a graphical application for digital forensic analysis that runs on the top of Sleuth Kit. Using M3 it is possible to conduct a thorough analysis of forensic images created with help of FTK Imager tools. Analysis is also carried out on file systems; data is recovered and its metadata can be reviewed through the help of Autopsy. It supports a variety of file systems and formats and permits the forensic specialists to perform it work effectively. Features are timeline analysis, keyword search, and the possibility of obtaining detailed reports on the selected case.

Analysis Steps

Section	Description	Answer
Question 1	Evidence left behind on the system	Reasons that can remain in the system Reasons that can remain in the system consists of artifacts like file meta-data, system log-data and User activity traces. These artifacts can contain a lot of information about the user's activity, the time of file

		creation, modification or access, details about executed commands or applications. Such artifacts can be retrieved and analyzed by tools including FTK Imager and Autopsy to enable reconstruction of users' activities.
Question 2	Issues raised by EFF (Electronic Frontier Foundation) and EPIC (Electronic Privacy Information Center)	Points other stakeholders have raised EFF and EPIC are organizations that concerns with privacy and government surveillance ways; Some of the ways it raises issues include data collection, user consent and data protection ways. it mainly looks at the ways through which the government and the corporations affect privacy and civil liberal through data invasions. These matters may for example involve disagreement on the propriety of the required levels of privacy and data handling of one's information.
Question 3	Issues raised in the two papers (details not specified)	Question 3 As far as anti-forensics is concerned, the common issues dealt in the two papers (not described in detail) The issues that are typically dealt in the anti-forensics' papers include ways of how data is masked or erased to avoid being forensically retrieved. Such methods include data deletion, encryption, and the other tools

		typically known as counter-forensic tools aimed at making it data recovery impossible or at least challenging. These papers focus on the efficiency of these approaches and it ramifications which are dear to forensic research.
Question 4	Removal of evidence and differences between issues raised by EFF/EPIC and anti-forensics papers	Question 4: Techniques that could be used to eliminate evidence and differences between issues highlighted by EFF/EPIC and anti-forensics papers Techniques used to remove evidence entails the act of deleting or altering all the evidential biomarkers with a view of making it hard for forensic experts to conduct investigations. This involves techniques such as file erase, disk erase and generally any technique that results into damage or erasure of data. The differences between issues raised by EFF/EPIC and those in anti-forensics papers lie in it focus: EFF/EPIC fund and protect user rights and privacy and ethical issues accruing from data gathering and surveillance are its main concern, while anti-forensics are papers outlining ways of avoiding detection by executing tricks on data that might alert the invader.

Table 1: The Question Answer Table

There is a precise process of identifying and interpreting the data received as a result of the analysis of the forensic image. The following steps outline the detailed process for analyzing a forensic image:

Initial Examination and Verification

To commence the examination there is checking of the authenticity and correctness of the forensic image. This entails the comparison of hash values such as the MD5, SHA-1 or SHA-256 of the original evidence to that of the forensic image thus 'Hashing'. The verification process becomes confirmation that the image is an accurate representation of the actual data. This step is also important in the process of minimizing the alteration of the evidence and is recorded in the forensic process. Some programs like FTK Imager help in this through creating and checking of hash values as part of the imaging process.

File System Analysis

The next operation to be performed is the analytical examination of the file system after confirming the authenticity of the forensic image. This involves features such as the actual file names, the directories or sub-folders, and the entire metadata. In simple terms, metadata analysis has the objective of enumerating and classifying it based on the type of file, its location, and the presence of notable metadata (Fernando, 2021). Analysis of file systems enables one to see the structure of data and define areas that will be researched.

Recovered Files of Interest

The analysis of the forensic image showed the following files and information of interest (Lwin *et al.* 2020). These findings are quite important in appreciating the background and possible repercussions of the investigation. The key recovered files and details are described below: The key recovered files and details are described below:

Email Addresses

One of the most important findings of the forensic image was a database of email addresses. These addresses included notable contacts such as:

- steve mcintyre 93sam@debian.org
- azat khuzhin a3at.mail@gmail.com
- axel beckert abe@debian.org

Thus, it is possible to detect the presence of these email addresses in package files and other metadata such as the email logs.

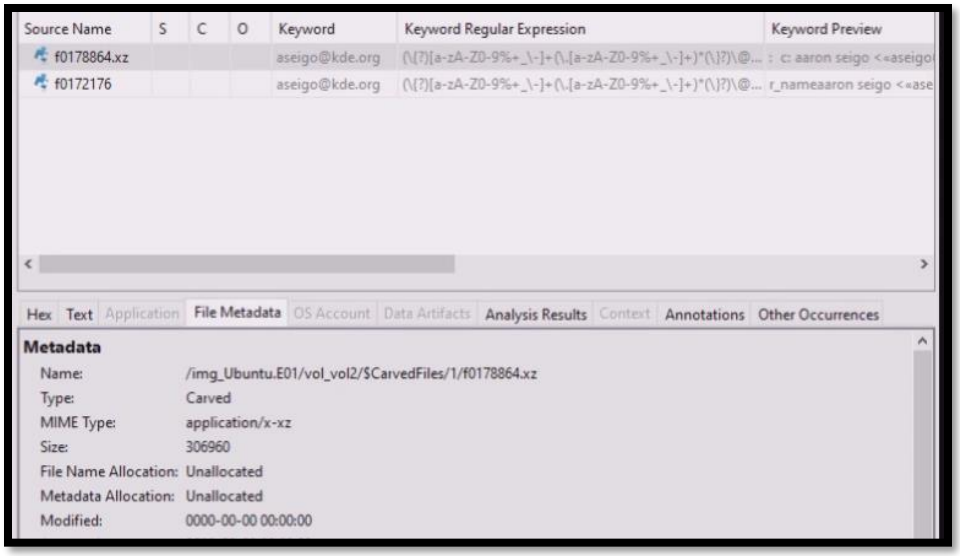

Figure 5: The File Metadata

(Source: Obtained from Autopsy)

These addresses imply that there could be possible lines of communication in relation to the case (Shafiee *et al.* 2023). Understanding under what circumstances these email addresses are used can help in the study of the content of the correspondence, the cooperation or other interactions related to the case.

Package Files

The forensic image contained several package files, including: The forensic image contained several package files, including:

o libunistr (files: ‘trading plan ‘& ‘strategic plan’ (f0145184.deb, f0699728.deb).

o libvorbis (files: (f0145184.deb, f0699728.deb)

These package files are related to certain software packages and were obtained from the allocated as well as unallocated clusters. By examining such files, one may get installation details, software and its versions, and also the changes that may have been brought on the system. Possibly, these packages relate to the software components or updates that can be relevant to the case under consideration.

File Metadata

Working with metadata of the given files proved to be insightful, as the obtained metadata included time stamps, file size and file path. Key findings include:

o File Creation Dates: Some of the files contained creation dates corresponding to the events on the case timeline.

o Access and Modification Dates: Examining the ‘access’ and ‘modified’ properties paved the way on configuring a time-line of the actions done by users and other possible changes to the files.

This metadata helps to restore the actions of the user and explain the circumstances in which it used or changed some files.

Logs and Documentation

- Recovered logs and documentation files included:
- o System Logs: Records the event histories that include situations occurring in the system, errors as well as user activities.
- o Documentation Files: Documents that have either instructions or information note about the software and the packages that were used.

These logs and documents provide information about the fundamental functioning of the system and the involvement of the users as well as the settings (Aburbeian *et al.* 2023). It is vital in deciphering the system utilization and areas of concern such as discrepancies that can be associated with the case.

Suspicious Files

Several files raised suspicion due to its content or context, including:

o Files with Unusual Extensions or Names: Some of these files had outstanding extension or name that was not a norm when it came to a particular file type or an expected file extension.

o Files Containing Sensitive Information: Some of the files had information that was either sensitive or looked confidential like user log in credentials or communication within the firm.

Seizing these files can reveal something that has been well hidden or encrypted, or any evidence of manipulation or other related information that may help in solving the case.

In brief, the relevant files which are retrieved are email addresses, package files, its metadata, logs & documentation, and other suspicious files (Grispos and Bastola, 2020).

2.3 Critical Reflection

Challenges Faced

When working on the imaging and analysis stage, numerous problems were identified that affected the investigation’s productivity and efficacy. These difficulties include:

Handling Corrupted Data

Corrupted or damaged files were a major issue The structure of the program was not as accessible as fully functioning files. Certain files within the forensic image were non-readable or non-openable which was as a result of corruption (Cristian *et al.* 2020).

Volume of Data

More, due to the number of files present in the obtained forensic image, which contained pornographic images and videos, this was proven to be a challenge (Žulj *et al.* 2020). Due to the total number of files and it metadata, there was a need to process and sort large amounts of information. Determining what files are important out of all the documents needed was a delicate process of outlining which data to look for and the right utilization of the available instruments in order not to lose certain important data.

File Fragmentation

Due to the fact that the files were fragmented to different sectors of the image, reconstructing the image was very tedious. In segmented files areas of the file were stored in different blocks in the image and file had to be compiled from these areas (Young *et al.* 2021). This fragmentation, however, labeled it difficult to get constant and coherent information from a few files.

Data Obfuscation

Such cases of data masking were observed and it include files with unconventional extensions and content that had been encrypted (Al-Faaruuq and Priambodo, 2022). Overlaid or actually encrypted files for further camouflage had to be searched and, in some cases, decoded.

Tool Limitations

It was a limitation that the tools which were applied in the forensic process, such as FTK Imager and Autopsy had its respective limitations. Al though these tools are effective on one hand it offers specific functionalities on the other hand.

Learning Outcomes

Based on the exercise, these are the conclusions that would be derived from the case as it relates to the learning outcomes of the course in digital forensics:

First of all, the necessity of strict correspondence to the rules for making a force by employing the forensic imaging was discussed. Monitoring the image's quality was a critical objective in this case to guarantee that the procedures followed in handling the evidence were proper and reliable (Salamh *et al.* 2021).

Secondly, it was identified that the tasks of analyzing immense amounts of data were not as simple as it was initially imagined. Appropriate data management and more specifically, efficient filtering of the large data streams or databases was also indispensable for sourcing and filtering relevant information. In this context, the forensics carved out the need of sound organizational measures and efficient applicative use of forensic tools. Further, difficulties arising with file fragmentation and data masking described the deficiencies of forensic instruments and the requirement for extra methodologies (Azo 2013, Lowetz *et al.* 2024).

Suggestions for Improvement

As for the studies of the future, the following recommendations can improve the effectiveness and efficiency of the forensic process.

First of all, the increase of using sophisticated forensic tools and technology can enhance the general data recovery and analysis. Using the advanced versions of the software known to have better features for data extraction and analysis as well as handling of cases can more effective.

Secondly, it is recommended that agencies adopt a protocol for postmortem photography and imaging/interpretation. Adherence to standardized methods in the various investigations help in elimination of variations and hence errors which ultimately enhance reliability of the evidence. Having a set of guidelines and checklists will help the organization stick more to the best practices in each step of the process.

Lastly, more elaborate review and validation of the identified findings cut reduce chances of the above oversight. The analyzed data and results are more accurate with the aid of extra verification checks and peer reviews do not miss important pieces of evidence.

3. Conclusion

The forensic examination showed unique features both in the findings regarding the digital evidence. The investigation was carried out in the following order: making a forensic copy by FTK Imager software and comprehensive examination with the help of Autopsy application. It should also be noted that the systematic approach meant there was no loss of data – a factor very important in the analysis. Some of the discoveries that the analysis yielded include several possible email addresses and files that provided information on the events and communications that have been recorded in the digital evidence. This way, the elements highlighted gave relevant information in relation to the goals and objectives of the investigation. Some of the problems that were met during the process are connected with technical side like data extraction, and semi-automatic data analysis which might be considered as nontrivial task due to the fact that some of the formats of files were quite difficult to interpret.

4. References

Shafiee, M.Z.A.B., Ali, F.H.B.M. and Zulkipli, N.H.B.N., 2023, December. Linux Forensic Analysis and Extraction Tool. In *2023 IEEE 8th International Conference on Recent Advances and Innovations in Engineering (ICRAIE)* (pp. 1-5). IEEE.

Cristian, P.C., Hernan, T.C., Rene, G.Q., Francisco, A.P. and Cristian, N.G., 2020, June. Methodologies and Forensic Analysis Tools on Android Mobile Devices: A Systematic Literature Review. In *2020 15th Iberian Conference on Information Systems and Technologies (CISTI)* (pp. 1-7). IEEE.

Young, E.H., Chrysoulas, C., Pitropakis, N., Papadopoulos, P. and Buchanan, W.J., 2021, October. Evaluating tooling and methodology when analysing bitcoin mixing services after forensic seizure. In *2021 International Conference on Data Analytics for Business and Industry (ICDABI)* (pp. 650-654). IEEE.

Salamh, F.E., Mirza, M.M., Hutchinson, S., Yoon, Y.H. and Karabiyik, U., 2021. What's on the horizon? An in-depth forensic analysis of android and iOS applications. *IEEE Access*, *9*, pp.99421-99454.

Al-Dhaqm, A., Abd Razak, S., Ikuesan, R.A., Kebande, V.R. and Siddique, K., 2020. A review of mobile forensic investigation process models. *IEEE access*, *8*, pp.173359-173375.

Lwin, H.H., Aung, W.P. and Lin, K.K., 2020, February. Comparative analysis of Android mobile forensics tools. In *2020 IEEE Conference on Computer Applications (ICCA)* (pp. 1-6). IEEE.

Grispos, G. and Bastola, K., 2020, July. Cyber autopsies: The integration of digital forensics into medical contexts. In *2020 IEEE 33rd International Symposium on Computer-Based Medical Systems (CBMS)* (pp. 510-513). IEEE.

Žulj, S., Delija, D. and Sirovatka, G., 2020, September. Analysis of secure data deletion and recovery with common digital forensic tools and procedures. In *2020 43rd International Convention on Information, Communication and Electronic Technology (MIPRO)* (pp. 1607-1610). IEEE.

Şentürk, Ş., Apaydın, T. and Yaşar, H., 2020, October. Image and file system support framework for a digital mobile forensics software. In *2020 Turkish National Software Engineering Symposium (UYMS)* (pp. 1-3). IEEE.

Fernando, V., 2021, April. Cyber forensics tools: A review on mechanism and emerging challenges. In *2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS)* (pp. 1-7). IEEE.

Shobana, G., 2021, May. The State of the art tools and techniques for remote digital forensic investigations. In *2021 3rd International Conference on Signal Processing and Communication (ICPSC)* (pp. 464-468). IEEE.

Ozcan, S., Astekin, M., Glisson, W.B. and Choo, K.K.R., 2021, October. DIEF: An Autopsy Module for Distributed Identification of E-mail Files from Disk Images. In *2021 IEEE 9th International Conference on Smart City and Informatization (iSCI)* (pp. 53-61). IEEE.

Al-Faaruuq, M.S. and Priambodo, D.F., 2022, November. IOS digital evidence comparison of instant messaging apps. In *2022 International Conference of Science and Information Technology in Smart Administration (ICSINTESA)* (pp. 83-88). IEEE.

Hweidi, R.F.A., Jazzar, M., Eleyan, A. and Bejaoui, T., 2023, July. SATA M. 2 on Forensics: Trim Function Effect on Recovering Permanently Deleted Files. In *2023 International Conference on Smart Applications, Communications and Networking (SmartNets)* (pp. 1-6). IEEE.

Aburbeian, A.M., Owda, M. and Owda, A.Y., 2023, August. Digital Forensic Analysis of Hologram Projection Fans. In *2023 International Conference on Information Technology (ICIT)* (pp. 7-12). IEEE.

Lowetz, C., Shepard, G. and Coffman, J., 2024, April. Anti-forensics Under Scrutiny Assessing the Effectiveness of Digital Obfuscation in the Cloud. In *2024 12th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1-6). IEEE.

Arrizki, D.J., Kosim, S.A. and Studiawan, H., 2024, April. Stream Clustering on a Forensic Timeline. In *2024 12th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1-6). IEEE.