AN EXTENDED CFTT EVALUATION FRAMEWORK FOR FORENSIC TOOLS IN SOCIAL MEDIA INVESTIGATIONS

By

Ayesha Binte Aziz

MSIS-2019 : 00000319486

Supervisor

Dr. Mehdi Hussain

Department of Computing

A thesis submitted in partial fulfillment of the requirements for the degree of

Master of Science in Information Security in Education (MS IS)

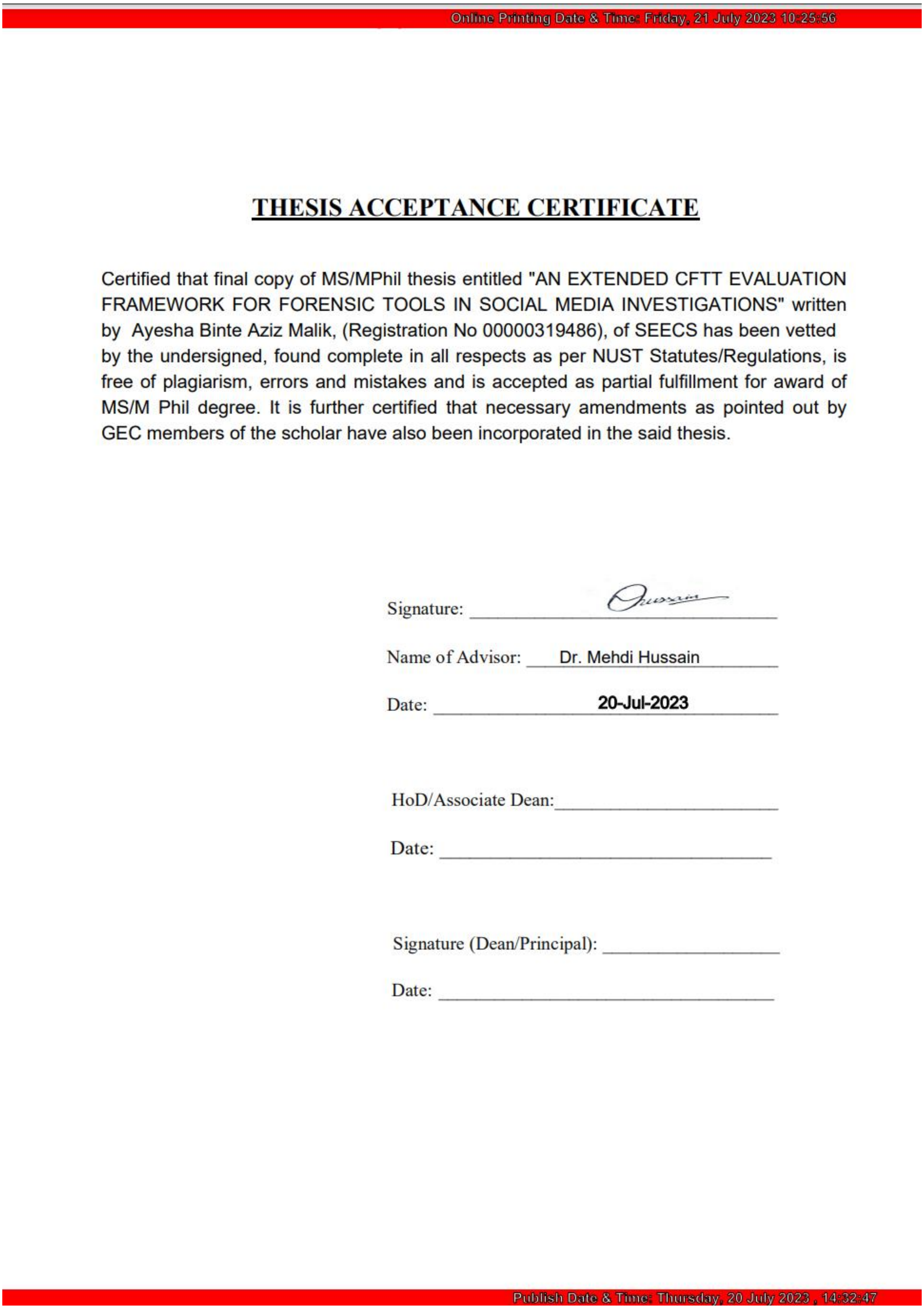
In

School of Electrical Engineering and Computer Science,

National University of Sciences and Technology (NUST),

Islamabad, Pakistan.

(July 2023)



Online Printing Date & Time: Friday, 21 July 2023 10:25:56

THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS/MPhil thesis entitled "AN EXTENDED CFTT EVALUATION FRAMEWORK FOR FORENSIC TOOLS IN SOCIAL MEDIA INVESTIGATIONS" written by Ayesha Binte Aziz Malik, (Registration No 00000319486), of SEECS has been vetted by the undersigned, found complete in all respects as per NUST Statutes/Regulations, is free of plagiarism, errors and mistakes and is accepted as partial fulfillment for award of MS/M Phil degree. It is further certified that necessary amendments as pointed out by GEC members of the scholar have also been incorporated in the said thesis.

Signature: Hussain

Name of Advisor: Dr. Mehdi Hussain

Date: 20-Jul-2023

HoD/Associate Dean: ______________________

Date: ______________________

Signature (Dean/Principal): ______________________

Date: ______________________

Publish Date & Time: Thursday, 20 July 2023 , 14:32:47

Online Printing Date & Time: Friday, 21 July 2023 10:26:15

Approval

It is certified that the contents and form of the thesis entitled "AN EXTENDED CFTT EVALUATION FRAMEWORK FOR FORENSIC TOOLS IN SOCIAL MEDIA INVESTIGATIONS" submitted by Ayesha Binte Aziz Malik have been found satisfactory for the requirement of the degree

Advisor : Dr. Mehdi Hussain

Signature: Hussain

Date: 20-Jul-2023

Committee Member 1:Dr. Dr Hasan Tahir

Signature:

20-Jul-2023

Committee Member 2:Dr. Muhammad Khuram Shahzad

Signature: MKhurram.

Date: 20-Jul-2023

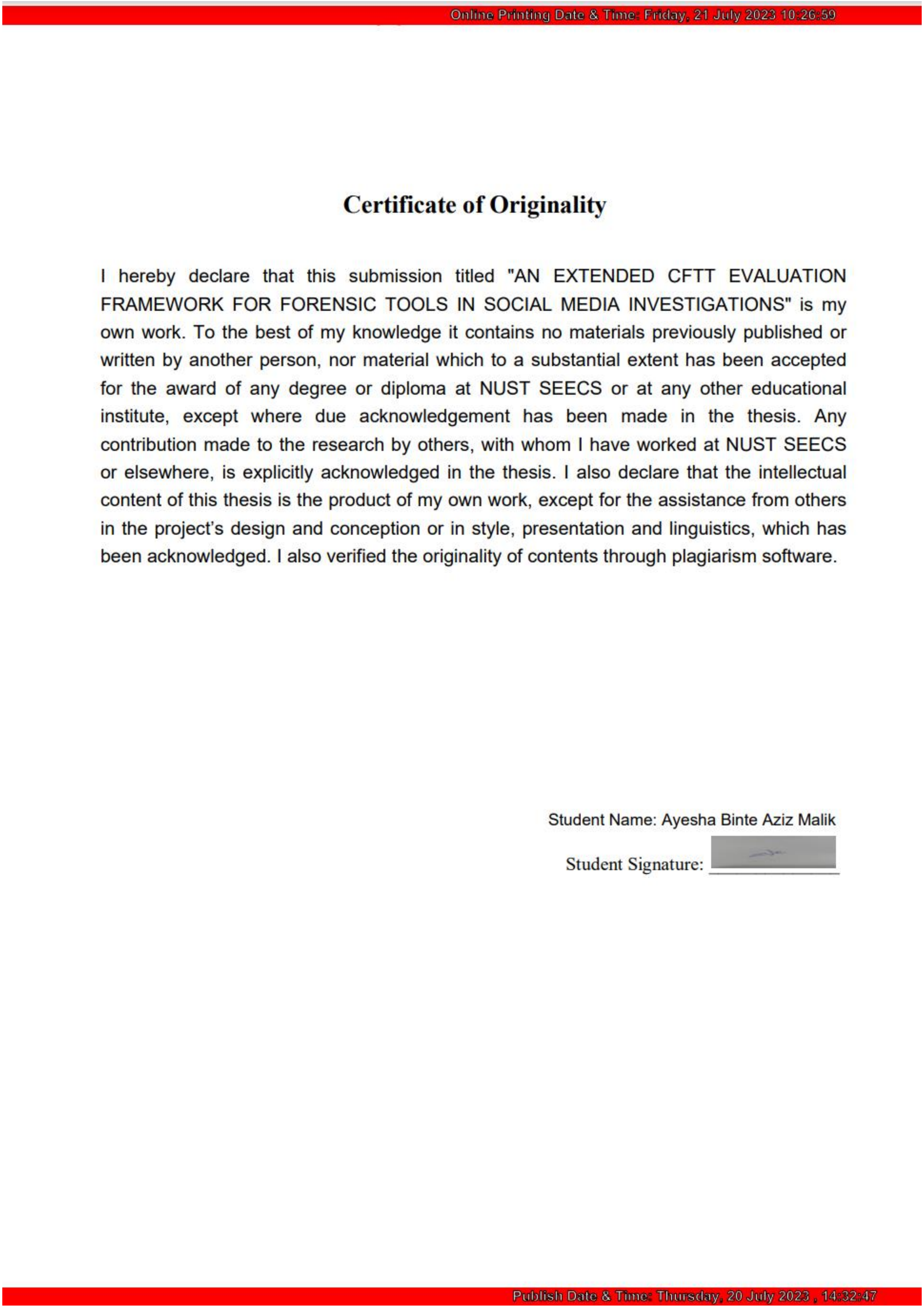
Signature: ______________________

Date: ______________________

Publish Date & Time: Thursday, 20 July 2023 , 14:32:47

Dedication

Dedicated to my parents for their unconditional love, prayers, and support throughout my life; my siblings, especially my brother whose support and help in everything makes life easier.



Online Printing Date & Time: Friday, 21 July 2023 10:26:59

Certificate of Originality

I hereby declare that this submission titled "AN EXTENDED CFTT EVALUATION FRAMEWORK FOR FORENSIC TOOLS IN SOCIAL MEDIA INVESTIGATIONS" is my own work. To the best of my knowledge it contains no materials previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any degree or diploma at NUST SEECS or at any other educational institute, except where due acknowledgement has been made in the thesis. Any contribution made to the research by others, with whom I have worked at NUST SEECS or elsewhere, is explicitly acknowledged in the thesis. I also declare that the intellectual content of this thesis is the product of my own work, except for the assistance from others in the project's design and conception or in style, presentation and linguistics, which has been acknowledged. I also verified the originality of contents through plagiarism software.

Student Name: Ayesha Binte Aziz Malik

Student Signature: ______________

Publish Date & Time: Thursday, 20 July 2023 , 14:32:47

Acknowledgement

First and foremost, praises and thanks to the Almighty Allah, for His showers of blessings throughout my life.

I would like to thank my research supervisor Dr. Mehdi Hussain for his guidance throughout my research and helping me whenever I was lost.

I am extremely grateful to my parents for their love, prayers, care and sacrifices for educating and preparing me for my future. Also, I express my thanks to my brother for his support and valuable prayers.

Table of Contents

List of Abbreviations

NIST – National Institute of Standards and Technology

CFTT – Computer Forensic Tool Testing

CA – Core Assertion

AO–Optional Assertion

CR–Core Requirement

OR–Optional Requirement

MDT– Mobile Device Tool

SPN – Service Provider Name

ICCID–Integrated Circuit Card Identifier

IMSI– International Mobile Subscriber Identity

MSISDN– Mobile Station International Subscriber Directory Number

ADNs– Abbreviated Dialing Numbers

LND–Last Numbers Dialed

UTF–Unicode Transformation Format

List of Tables

List of Figures

Abstract

Smartphones and Social media applications are particularly prominent in their usage and are often utilized for criminal purposes. Although several mobile forensic tools are available for investigation, it becomes challenging for investigators to select the most suitable tool capable of analyzing different types of social media apps with all available features. Furthermore, there is a lack of a detailed evaluation framework to assess the capability of forensic tools in examining social media apps. In this context, this study aims to propose a social media forensic framework along with 151 test cases. The proposed framework builds upon the CFTT mobile forensics tools evaluation framework. For the experiments, three open-source tools, namely Autopsy, Andriller, and AFLogical, are used, while the social media applications WhatsApp, Telegram, and KalamTime are employed. The experimental strategy consists of three phases. First, various user activities are performed on social media applications. Second, device images are obtained both with and without rooting the devices. The acquired images are then forensically analyzed using the selected tools. Finally, the forensic tools are evaluated based on the proposed test cases. Autopsy had a success rate of 56% for test cases involving built-in mobile features. Regarding social media applications, Autopsy achieved 67% for WhatsApp, 41% for Telegram, and 56% for KalamTime. Andriller, on the other hand, had a success rate of 42% for built-in mobile features and 59% for WhatsApp's social media application. Telegram and KalamTime had success rates of 6% and 4%, respectively. AFLogical succeeded in 14% of the test cases for mobile devices, but it couldn't find any evidence related to social media applications using the proposed test cases.

In the future, the proposed test cases can be analyzed on other existing social media apps and forensics tools for broader comparison.

Keywords: Mobile Forensics, Tool Testing, Evaluation Framework

1. Introduction

1.1 Background

Mobile forensics is a relatively new sub-discipline of digital forensics, that started in the late 1990s. It hasn't gotten as much attention as some of the more well-known sub-disciplines in this area, like network forensics, database forensics, and firewall forensics.

Mobile forensics is challenging due to different kinds of mobile devices from different manufacturers coming into the market. Mobile phones have also evolved from simply calling and texting to email, internet surfing, using a variety of applications, and many other activities. Mobile devices are being used on a large scale and are consequently being used in criminal activities as well [38]. This situation has increased the demand for forensic investigation of mobile devices. Important data such as contacts, call logs, SMS, MMS, and calendar can be retrieved using mobile device forensics. Additional data such as email, browsing history, and social media application data can be retrieved in case of smartphone forensic investigations.

The use of social media applications via smartphones has also become very common. 4.80 billion active social media users were recorded in 2023 [3]. Various industries such as the fashion industry, entertainment industry, tech industry, music industry, and other businesses are benefiting from social media [4]. Consequently, the use of social media applications in criminal activities has also increased, such as theft of personal information, stalking, cyberbullying, and harassment. Therefore, forensic analysis of social media applications has also become a necessity. Different artifacts collected from smartphones can be used as digital evidence in court cases and criminal prosecutions.

1.1.1 Digital Forensics

Digital forensics involves acquiring, processing, analyzing, and reporting digital data obtained from digital devices such as computers, tablets, storage devices, mobile phones, and cloud storage [5]. This digital data is digital evidence that can be used in a criminal case. Digital evidence refers to any digital information that can be presented as evidence in court.

Various artifacts such as documents, media files, call logs, SMS, timestamps, and location can be used as digital evidence. Various digital forensic software is available for forensic analysis of digital devices. Both commercial and non-commercial tools are available such as EnCase® Forensic, F-Response, Forensic Toolkit, Autopsy, Forensic Investigator, and others [6, 7]. For example, EnCase® provides in-depth acquisition of evidence, various customization options for the ease of investigator, and detailed reporting [8]. Such tools provide ease for a forensic investigator to collect and analyze digital evidence.

1.1.2 Mobile forensics

Mobile forensics is a sub-discipline of digital forensics in which electronically stored data within mobile devices is retrieved and analyzed for forensic purposes [9]. In mobile forensics, there are two types of data acquisition techniques:

- **Logical acquisition techniques** in which data within the allocated space of a mobile device is acquired, i.e., bit by bit copy of the used space. However, the remaining bits occupying the free space are not acquired. If there is any deleted data present in the slack space, it cannot be recovered using logical acquisition techniques. To apply these techniques, the device does not need to be rooted and only USB debugging mode is required to be enabled, although in contrast to physical acquisition the data retrieved is less [10].

- **Physical acquisition techniques** in which bit by bit copy of the whole physical storage of a mobile device is acquired, i.e., both allocated and unallocated space are copied. The extensive size of data can be recovered as compared to the logical acquisition, such as deleted documents, videos, images, messages, etc. However, physical acquisition requires the rooting of a device. This rooting process makes the device void of warranty, vulnerable to malware and the device can be bricked if not rooted correctly [10].

The processes involved in mobile forensics, according to the National Institute of Standards and Technology (NIST) are:

- **Preservation** involves securing, analyzing, and documenting the scene, collecting and storing the evidence, determining the urgency of the incident, and making an on-site decision tree that will help analyze the case.
- **Acquisition** involves initially identifying the mobile device details, choosing the relevant mobile forensic tools, and performing logical and physical acquisition, depending upon the case.
- **Examination and analysis** involve separating relevant information after the data is exposed, applying the selected tools and performing analysis, and gathering all records.
- **Reporting** involves documenting and presenting all the actions performed in the forensic investigation and reporting the results in detail.

Holistically, mobile forensics answers the following questions [10]:

- What is the nature of the case?
- What is the primary goal of the investigation?
- In what period did the series of events take place?

- What kind of evidence might be used to prove or disprove the hypothesis?
- What relationship is there between the mobile forensic data and the other digital and non-digital evidence?

1.2 Motivation

The number of smartphone users and correspondingly social media app users is increasing rapidly. In addition to local calls and SMS, people are using apps like WhatsApp, Telegram, and WeChat to make calls, send messages, share media files, share locations and use various features that these apps provide. Consequently, digital crime involving social media has also become common. Various cases can be formed and solved based on evidence collected from the usage of these apps.

Several cases have already been solved based on digital evidence collected from the use of social media apps. In 2019, the claimants from Secarma Ltd accused the defendants of poaching their employees [11]. When the case was filed, there had been 28 resignations already. According to the claimants, the purpose of poaching their employees was to move them to a competitor company that was working on pen testing in competition with Secarma Ltd. The evidence presented by Secarma Ltd was WhatsApp messages exchanged in a group chat in which it was planned to poach the employees from Secarma Ltd [11].

Similarly, social media has been used for crimes on a larger level, for example promoting graphic violence, mob violence in Sri Lanka and Bangladesh, ethnic and religious conflict in India, and the abuse of blasphemy laws in opposition to religious minorities in Pakistan [12].

Various mobile forensic tools are available online for ease of use by a forensic investigator. Several commercial/non-commercial tools are available. But it is difficult for an investigator to choose which tool to use in case of a digital crime. An evaluation of these tools is required so that the forensic investigator can choose a tool according to its performance and functionality. This research work will evaluate mobile forensic tools according to Mobile device tool test specification guidelines presented by the Computer Forensic Tool Testing (CFTT) project of NIST. These guidelines present requirements of a tool, test assertions, and test cases for evaluation.

Once a mobile device has been analyzed forensically, the evidence presented by the tool shall be admissible in court.

This research work proposes test cases extended from test assertions provided by the CFTT evaluation framework to assess open-source mobile forensic tools, and also assess them on their ability to forensically analyze social media application data.

This can help a forensic investigator to select a tool wisely. It also helps developers make needed improvements in their tools in addition to setting a benchmark for tool validation, admissibility, and standardization.

1.3 Problem Statement

With the extensive usage of social media applications on smartphones, cybercriminals have plenty of opportunities to commit cybercrimes via these applications. The requirement of forensic analysis of mobile phones including detailed analysis of social media applications has been raised. Several mobile forensic tools have been developed for the ease of a forensic investigator. However, there is a lack of specialized forensic tools designed to evaluate different kinds of popular social media applications. Further, there is also a lack of evaluation of these existing forensic tools according to NIST CFTT standardization, especially for social media application data analysis.

Different frameworks exist for the evaluation of mobile forensic tools, but advanced frameworks are required that can evaluate a forensic tool based on its ability to forensically analyze social media application data and make the decision of selecting a tool easier for an investigator.

1.4 Research Objectives

This research work aimed to make the choice of selecting forensic tools (on their ability to analyze social media applications) easier for an investigator. The objectives of the study are mentioned below:

a) Identify artifacts of the selected social media applications that can be used as digital evidence in court.

b) Create test cases for social media applications to evaluate a forensic tool.

c) Evaluate the selected open-source mobile forensic tools using the evaluation framework provided by CFTT and the proposed test cases, which include requirements, test assertions and test cases.

1.5 Scope

Three mobile forensic tools were chosen for this research work. The criteria for choosing these tools were that they are open-source and free. The tools chosen were Autopsy, Andriller, and AFLogical. Three social media applications were chosen for forensic analysis, namely WhatsApp, Telegram, and KalamTime. The criteria for choosing them were their popularity and common features. The scope of this research is:

- The scope of this research is limited to three open-source mobile forensic tools.
- Only the selected social media applications were forensically analyzed.
- Windows 10 will be used for testing environment.

- The rooted device used for forensic examination was Samsung Galaxy Grand Prime, Android Version: 5.0.2, Model: SM- G530H.
- The un-rooted device used for forensic examination was OPPO F9, Android Version: 10
- The device was rooted for physical image acquisition and other tools that played roles in the acquisition of physical image were BusyBox Utility, KingoRoot App, ADB Utility, and NCAT Utility.
- Additional Test Cases were added according to the assertions provided by CFTT documentation.

1.6 Summary

This chapter covered the background of mobile forensics and digital crimes at the beginning. Next, it gave an insight into digital forensics and mobile forensics. The processes provided by NIST for mobile forensics were presented later. After this, the motivation, problem statement, and scope of the thesis were discussed.

2. Literature Review

2.1 Overview

Mobile forensics is becoming popular among researchers in recent years. It is generally because of the increase in cyber-crimes with the vast use of mobile devices, especially with social apps. Different kinds of applications and especially interactive applications have come into the market such as social media apps, dating apps, gaming apps involving communication, and many other kinds. Online interaction can lead to criminal activities such as cyberbullying, harassment, drug dealing, hacking user accounts, robbery of families during vacation [13], and many more.

In the research involving mobile forensics, recent studies have proposed mobile forensic tools [14, 15]. Comparative analysis of existing forensic tools has also been performed [16, 17, 18]. Popular interactive applications have been analyzed as well using available forensic tools [19, 20]. Each study opens up the path to future studies because applications and forensic tools keep getting updated frequently, requiring more research

Popular social media applications have been analyzed from a forensic perspective so that they can help a forensic investigator investigate a crime related to that particular application. Different challenges that researchers have experienced in this regard involve difficulty in rooting a device, inability to extract all forensic evidence, the tool being used for forensic analysis not being enough for artifact extraction, and difficulty in recovering deleted data.

2.2 Related work

In this section, the related literature is presented. Using already available forensic tools and the latest tools proposed in the literature, popular Smartphone applications, desktop applications, duplicate applications, and PC applications have been forensically analyzed in the current literature.

2.2.1 Forensic Analysis of Smartphone Cloud Applications:

Bhat et. al. [20] examined cloud applications namely Sync.com and FlipDrive. The forensic examination was performed using dd utility and Hex workshop. The research revealed that plenty of information was left in the mobile when user activities were performed. Mechanisms to recover digital evidence were also identified and presented in this study. Login credentials, timestamps of activities, names, and locations of files, and several other related data were recovered and a digital investigator could create complete file management logs by using this research methodology. On the downside, only limited deleted data was recovered and in future studies more tools could be used to recover deleted data and also artifacts related to sharing applications.

2.2.2 Forensic Analysis of Social Media Applications:

Pribadi et. al. [19] performed a forensic analysis of the Facebook messenger application. The forensic analysis was carried out using MOBILedit Forensic Express PRO. In this study, the author employed an unrooted device due to which chat and audio could not be recovered. Videos, photos, and application information was recovered that can be used as digital evidence in court. Future studies could use a device in a rooted state for detailed artifacts recovery and a comparison could be done between forensic tools for better examination of social media applications.

Shreya et. al. [21] performed a forensic analysis of the Instagram application and highlighted the feature of disappearing messages. MSAB XRY and XAMN were used for the forensic analysis of Instagram. The research successfully discovered the presence of vanished messages in the Instagram database. It also pointed out some inconsistencies regarding data of vanished messages in the application database. The study also presented how the media uploaded by the user is stored. The keywords used in the search bar and shopping tab were recovered. Future research in disappearing media was recommended. It was also suggested by [21] to research how personal media is stored during vanish mode. Personal identification artifacts also needed more research and the way they are stored by Instagram.

Mahr et. al. [22] conducted a forensic examination of the Zoom application using various forensic tools namely Magnet Acquire, Autopsy, ADB, and SQLite DB Viewer. The research was done after the popularity of Zoom during the Covid-19 Pandemic, and various incidents related to Zoom bombing. A great number of artifacts were recovered from the Zoom application during this study, such as email addresses, chat messages, passwords, and many more. Memory forensics, Network capturing and images of devices were taken to extract zoom artifacts. Some activities such as deleting contacts were also marked as possible anti-forensics on some platforms. Continuous and fast updates of Zoom require more research of the latest version, and other video conferencing applications could also be forensically examined in the future.

Nghi et. al. [23] performed a forensic examination of the popular TikTok application using ADB utility and SQLite DBViewer. A significant number of artifacts related to TikTok were recovered such as user's messages, likes, search keywords, etc. The artifacts were also explained by describing them in detail separately. This research was limited to the Android platform, and further research was recommended for the iOS platform.

Menahil et. al. [24] performed a forensic analysis of five social networking applications Instagram, LINE, Whisper, WeChat, and Wickr using three forensic tools namely Magnet AXIOM, XRY, and Autopsy. Most of the artifacts were successfully recovered in this study. The forensic tools were also compared based on their forensic capabilities. Magnet AXIOM was found to be the most effective forensic tool among the three other tools. For future work, newer versions of Android were recommended for analysis. It was also recommended by [24] that several forensic tools should be used as different tools have different capabilities.

Kim et. al. [25] selected two instant messaging applications with secure communication features, namely Wickr and private text messaging (PTM), for forensic analysis. Static and dynamic analyses were performed after acquisition using ADB utilities. As these applications store data in an encrypted format, decryption was done and verified via simulations. Analysis of Wickr was performed for both Android and iOS platforms. As PTM was not analyzed on iOS, hence in future research it could be decrypted and analyzed.

Mahendra et. al. [30] used MOBILedit Forensic Express to forensically analyze the Michat app to identify any illegal activities being carried out through the app. National Institute of Justice (NIJ) methodology was used for this study. The artifacts obtained including traces of chat could be used as digital evidence in court. They used a single well-known forensic tool for analysis, although more tools could be used for detailed forensic analysis. In the future, similar applications can be analyzed to provide detailed insight into these applications and benefit a forensic investigator analyzing such an app.

Ichsan et. al. [31] used multiple tools such as MOBILedit Forensic Express pro, BelkaSoft Evidence Center, DB Browser and Accessdata FTK Imager for forensic analysis of IMO messenger on android platform. Both rooted and unrooted devices were used for testing. A narcotics case study was used for research. Digital Forensics Research Workshop Plenty of artifacts that can be used as digital evidence were found such as chat files, videos, images, audio, etc. MOBILedit forensic express proved to be the most effective forensic tool in this study. No evidence could be obtained in smartphones without roots. In the future, an updated version of IMO messenger can be analyzed and other applications can also be analyzed using the research methodology of this paper. Along with Android, the apps can be analyzed on iOS devices also.

Prayogo et. al. [32] performed forensic analysis of Signal Instant messenger using MOBILedit Forensic Express pro, BelkaSoft Evidence Center, and DB Browser. They identified the repetition of specific words indicating cyberbullying. The reports from MOBILedit Forensic Express Pro yielded detailed results as compared to other forensic tools, pointing it out as an effective forensic tool for forensic experts. Deleted data could not be recovered. For future work, it was recommended to calculate the word weight of specific words to detect cyberbullying.

Gandhi et. al. [33] forensically analyzed the GroupMe application on both Android and iOS platforms. Plenty of artifacts were recovered that could be used as digital evidence in court. In the device chosen, physical extraction did not exceed after many attempts, due to which it was concluded that this hurdle might face by the forensic analyst also if devices like these that don’t grant rooting permissions are at hand. Axiom and Ufed were used for forensic analysis of the GroupMe application. In the future, the work can be extended by analyzing the Desktop or Web client of the GroupMe application.

Barros et. al. [28] performed a forensic analysis of the Bumble app. The research described the way Bumble data was organized in the mobile device and the structure of the data. Artifacts that can be used as digital evidence were also extracted. Important artifacts such as the identity of the user and exchanged messages were retrieved. Files sent by a user could not be recovered in this study. As future work pictures and audio exchanged can be recovered. As the author developed a script presenting messages in PDF format, it was recommended to include it in the Autopsy browser in future studies.

2.2.3 Forensic Analysis of Desktop Applications:

Bashir et. al. [26] did a forensic examination of the LinkedIn Desktop application. Tools like Dumpit, WinHex, and FTK Imager were used and in-depth manual analysis was carried out. The manual analysis gave a detailed insight into artifacts as compared to the previous studies testing Windows store apps, according to the author. More Window Store applications becoming popular can be tested in the future to provide insight into the benefits of manual analysis. A comprehensive forensic tool can also be developed for an investigator to test this kind of application by analyzing the registry, RAM, and storage in detail.

Khalid et. al. [39] performed a forensic analysis of the Cisco WebEx Application. A detailed forensic analysis of memory, network, and disk space was carried out. FTK Imager was used along with manual analysis of the application. This study successfully recovered the various artifacts related to the Cisco WebEx application such as email addresses, profile photos, display names, video addresses, etc. For future research, the Web and Android versions of Cisco WebEx can be considered. Other videoconferencing applications can also be explored. More variables can be considered such as bigger memory, changing system loads, and different memory acquisition techniques.

2.2.4 Forensic Analysis of PC Applications:

Iqbal et. al. [27] performed application-specific forensics on a gaming communication app, namely Discord. Although it was found that Discord is not used by as many users as social media applications, its steady growth and some cyber-crimes led to its forensic analysis research. A forensic solution was proposed by the authors, namely ‘DiscFor’, that performed extraction, analysis, and presentation from of discord client side. This lessened the hustle of manual analysis for a forensic examiner and application-specific forensic tools were recommended for greater insight into the application artifacts. This research was limited to the PC version, in the future mobile application and web variants of Discord can be analyzed. Updated versions of PC applications can also be forensically analyzed in future studies.

2.2.5 Forensic Analysis of Duplicate Applications:

Faruk et. al. [29] researched how a duplicate and fake Covid-19 application can be identified. Several ways were presented to identify the malicious application, as such pirated apps exploit user data and some of them are also designed in an anti-forensic manner. The study showed that the package name of the app under test was randomly generated so that it can go undetected by simple examination, the app name and icon used were the same as the original one. The tools used to detect the suspicious application were android studio and a virtual emulator. The research was limited to only Covid-19 applications. In future studies, it can be proposed how duplicate social media applications can be identified.

Following table summarizes the above literature review:

Paper reference	Year	Forensic analysis tool	Application	Advantage	Limitation	Recommendations
[19]	2022	MOBILedit Forensic Express PRO	Facebook messenger application	Videos and photos were recovered as evidence.	Chat and audio could not be recovered.	Comparison of forensic tools for better examination Using rooted device for better insight
[20]	2019	dd utility, Hex workshop	Sync.com, Flip drive	Forensic investigators can see details of recoverable artefacts and their recovery mechanisms	Limited deleted data could be recovered	Use more tools to recover deletion and sharing operations artefacts
[21]	2021	MSAB XRY, XAMN	Instagram	Identification of vanished messages Detection of disappearing messages	The shopping feature was not explored in detail Testing not done on iOS device	Analysis of shopping feature Path identification of vanished messages on iOS device
[22]	2021	Magnet Acquire, Autopsy, ADB, SQLite DB Viewer	Zoom	Discovered security risks related to Zoom	Unable to keep up with Zoom's fast ongoing updates	Test updated version of Zoom Test further video conferencing applications
[23]	2020	ADB, SQLite DB Viewer	TikTok	Artefacts obtained could be further identified as digital evidence	Testing performed on the Android platform only	Other platforms, such as iOS need to be researched
[24]	2021	Magnet AXIOM, XRY, and Autopsy	Instagram, LINE, Whisper, WeChat, and Wickr	A large number of artefacts were extracted and categorized as potential evidence.	Very limited information was disclosed by Wickr.	Different popular applications can be tested with different versions of smartphones

[25]	2021	ADB Backup	Wickr, Private Text Messaging	The decryption of Wickr and PTM data	PTM was not tested on iOS	PTM could be decrypted on iOS devices.
[26]	2019	Dumpit, WinHex, FTK Imager	LinkedIn Desktop Application	In-depth manual analysis of artefacts resulting in more potential evidence as compared to previous studies	More applications could be tested to provide further insight into manual testing techniques.	Other trending window store apps can be tested A comprehensive tool can be developed
[27]	2021	Proposed by the author 'DiscFor'	Discord	Full data recovery by the proposed tool, No manual investigation of JSON or cache files is required because of reporting features.	Limited to PC application	Examination of mobile application and web variants Examination of discord application after updates
[28]	2022	Autopsy forensic browser, Frida, MobSF	Bumble	Significant bumble-related artefacts were found	Files sent could not be recovered	Recovery of pictures and audio Finding app's vulnerabilities Developing author's script to be included in Autopsy forensic browser
[29]	2020	Android Studio, Virtual emulator	Modified Covid-19 application	Several ways to identify suspicious applications were presented.	Limited to one application.	Ways to identify fake Social media applications.
[30]	2021	MOBILedit Forensic Express	Michat	Artefacts and traces of chat could be used as digital evidence.	More tools could be used for detailed forensic analysis.	Further Similar applications could be analysed for detailed insight.
[31]	2021	MOBILedit Forensic Express pro, BelkaSoft Evidence Centre, DB Browser, Accessdata FTK Imager	IMO messenger	Plenty of artefacts that can be used as digital evidence were found such as chat files, videos, images, audio etc.	Limited to the Android platform.	This research can be extended for more applications and updated versions of applications.
[32]	2022	MOBILedit Forensic Express pro, BelkaSoft Evidence Centre, DB Browser	Signal Instant Messenger	The reports from MOBILedit Forensic Express Pro yielded detailed results as compared to other forensic tools, pointing it out as an effective forensic tool for forensic experts.	Unable to recover deleted data.	Gather deleted data Calculate word-weight indicating cyber-bullying
[33]	2021	AXIOM, UFED	GroupMe	A substantial amount of "GroupMe" artefacts was recovered on the Android and iOS platforms.	Physical extraction was unsuccessful on the chosen device.	Extension of the analysis to Desktop or Web client of GroupMe application.
[39]	2021	FTK Imager	Cisco WebEx	Numerous artifacts related to Cisco WebEx were successfully recovered	Variables like changing system loads, different memory-acquiring techniques and the size of the memory were not considered.	Other platforms like Android and Web Versions can be forensically analysed. More Video conferencing applications can be tested.

Table 2.1- Summary of literature review

The literature review presented above implies that multiple digital forensic tools were used for the forensic analysis of different interactive applications. Most of the artifacts were recovered in the studies, but deleted data artifacts could not be identified in a few studies. Although forensic tools are utilized to extract and present application data, an investigator has to put strong effort to locate and analyze the output presented by the tools. Hence specialized forensic tools are required for social media applications for the ease of a forensic investigator. Some of the existing forensics tools are NIST compliance. However, there is a lack of standardization in the evaluation of forensics tools targeted for social media applications. In the next chapter, we will propose an extended CFTT-based framework while adding novel test cases for the evaluation of social media forensics tools.

2.3 Summary

This chapter covered the background and the related work of the thesis. The related literature has been presented along with a critical analysis of the studies. Previous research work and schemes used in the literature help in formulating the solution to the identified problem.

3. Research Methodology

3.1 Overview:

The evaluation of mobile forensic tools uses the conformance methodology of software testing. This methodology is based on design science [35]. Design science is a scientific problem-solving method used especially in Information Systems (IS) [34]. Artifacts related to information systems are designed and scrutinized to solve practical problems [34]. In this research, the problem of tool evaluation is solved using conformance testing.

The conformance testing method is adopted by the NIST project for tool testing called CFTT. The International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) Draft International Standard (DIS) 10641 defines conformance testing as a "test to evaluate the adherence or non-adherence of a candidate implementation to a standard" [36]. The understanding here is that if an implementation (e.g. software tools) fulfills certain requirements or specifications then it conforms to certain assertions that grant the tool a conformance indicator to validate its compliance with the acceptable standard. The tool undergoes a number of test cases in order to prove its compliance with these requirements and test assertions.

The methodology used for tool evaluation is based on conformance testing adopted by CFTT. Therefore, it will follow their steps and nomenclature of test requirements, test assertions, and test cases. Additional test cases will also be added according to each test assertion provided by CFTT. The step-wise method used for conformance testing is:

- Highlight all the requirements of the tools of a certain domain.
- Frame out the assertions based on the requirements.

- Develop all the test cases necessary for the conformance of each test assertion.

Conformance testing consists of the following steps.

- **Test Requirement/Specification:**

Test specifications are a set of requirements that a tool should have in order to qualify as a standard tool in the said domain. These requirements are developed by:

a) Research in the domain.

b) Vendor insights and knowledge.

c) Feedback from the consumers of the tools.

- **Test Assertion:**

A test assertion is a verifiable statement about a single condition after an action is performed by the tool under test [37].

- **Test Case:**

A test case usually checks an assertion after the action of a single execution of the tool under test [37]. The test cases are divided into core and optional test cases. Core test cases are carried out for every tool that is tested for that domain. Optional test cases are selected for every tool based on their offered features.

- **Conformance Indicator:**

The conformance statement is declared given the tool under evaluation complies with the test assertion that is being tested.

3.2 Proposed Methodology

The proposed methodology comprises several phases, including the selection of forensic tools and social media applications. The selection criteria for digital forensic tools involved considering only free or open-source options, while the selection of social media applications was based on their popularity. To evaluate the selected forensic tools, test cases derived from CFTT test assertions were employed. Initially, user activities specific to the chosen social media apps were identified. Once these activities were performed, a logical or physical image of the test device was acquired. The acquired image was then analyzed by the forensic tool, generating a report that was further examined to identify local mobile artifacts as well as social media artifacts. The obtained results were analyzed using the proposed test cases. Subsequently, a comparison of the forensic tools was conducted, and the comparative results were presented. The flow of proposed methodology is shown in Figure 3.1.

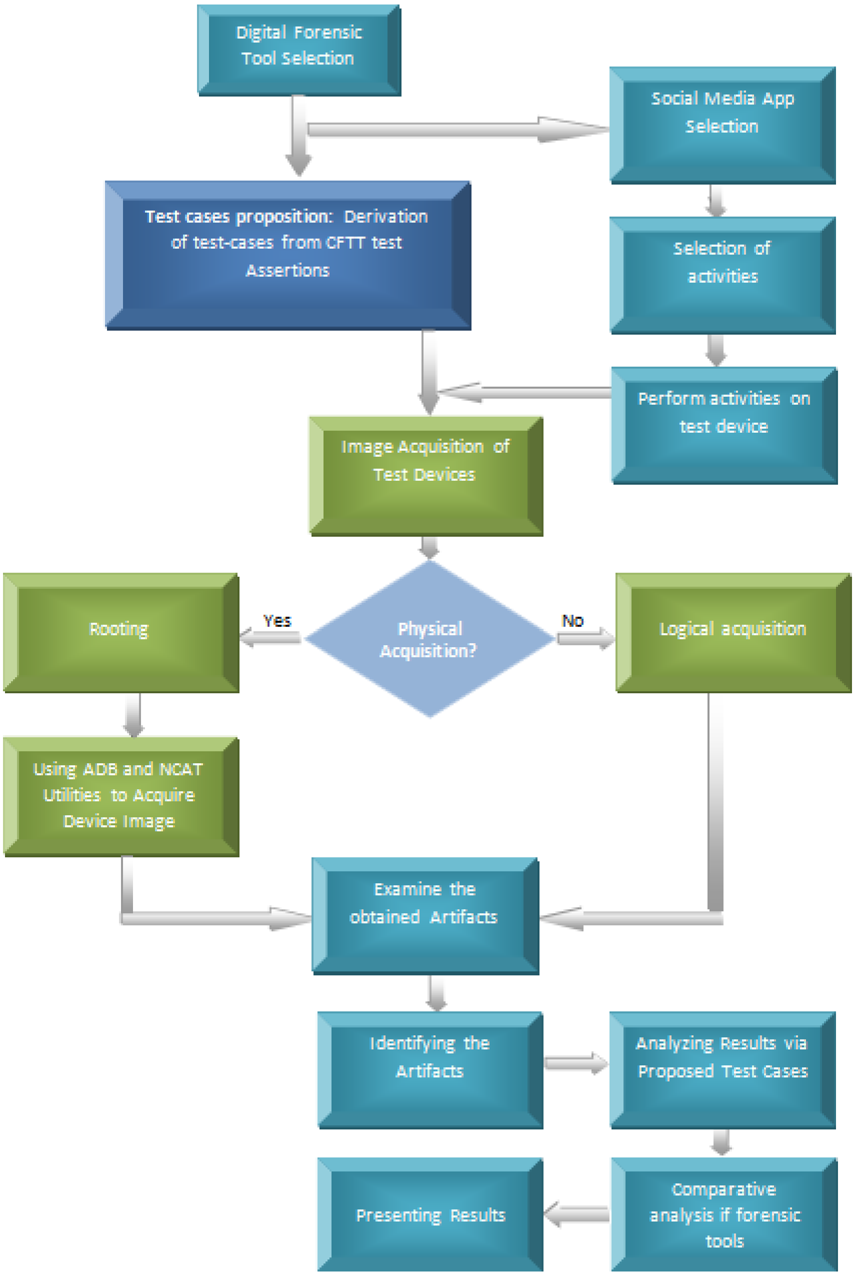

Digital Forensic Tool Selection
Social Media App Selection
Test cases proposition: Derivation of test-cases from CFTT test Assertions
Selection of activities
Perform activities on test device
Image Acquisition of Test Devices
Rooting
Yes
Physical Acquisition?
No
Logical acquisition
Using ADB and NCAT Utilities to Acquire Device Image
Examine the obtained Artifacts
Identifying the Artifacts
Analyzing Results via Proposed Test Cases
Presenting Results
Comparative analysis if forensic tools

Fig 3.1 – Flow of Proposed Methodology

3.2.1 Forensic Tools and Social Media Application Selection:

Three digital forensic tools, namely Autopsy, Andriller, and AFLogical were selected based on the tools being free and open-source. Next, three social media apps, namely WhatsApp, Telegram, and KalamTime were chosen based on their popularity and number of downloads.

3.2.2 Proposed Test Cases for CFTT Evaluation Framework:

CFTT Mobile Forensic Tool Evaluation Framework offers certain test requirements, test assertions, and test cases in order to evaluate a mobile forensic tool. Our proposed methodology offers an extended version of the CFTT Evaluation Framework in which additional test cases are added for forensic tool evaluation. Following the CFTT conformance methodology, when a forensic tool conforms to a test assertion, it successfully passes all the test cases that come under a given test assertion.

3.2.3 User Activities for Selected Social Media Applications:

Multiple user activities were performed according to the features provided by the selected social media apps. A lot of activities are common because of the similarity of the apps, but varying features also exist among the apps.

3.2.4 Test Device Image Acquisition:

After all the activities are performed, image acquisition of the test device is performed. In case a forensic tool accepts the physical image, the device under test needs to be rooted. Once a device is rooted, it is connected to the laptop being used under the test environment, then by using ADB and NCAT utilities, the device is allowed access, and its physical acquisition is performed. If a forensic tool accepts logical images only, then logical acquisition is performed.

3.2.5 Artifact Examination and Identification:

After the image acquisition, the forensic tool analyses the image and presents the results. These results are then examined and studied. Artifacts obtained are identified from the presented results.

3.2.6 Assessment via Proposed Test Cases:

Then the overall results are assessed via the proposed CFTT Framework-based test cases. The performance of a forensic tool is measured by its success or failure in a test case. After analyzing the overall performance of each forensic tool, their comparative analysis is performed to check which forensic tool performed the best. Finally, overall comparative results of the forensic tools are presented against each test case.

3.3 Summary:

This chapter covered the methodology followed by this research. CFTT conformance testing steps are explained as test cases extended from CFTT test assertions are a part of the proposed methodology. The proposed methodology is first presented in the form of a diagram and then each step is explained in table format.

4. Proposed Test Cases for CFTT Framework

This section will discuss the proposed extended CFTT-based framework for social media applications with novel test cases. In the beginning, the profiles of mobile forensics tools are provided. Next, the nomenclature used in the standard CFTT document is defined and the profiles defined are mapped to the test requirements mentioned in the CFTT document. Next, the proposed extended CFTT-based framework is presented.

4.1 Profiles

The requirements, test assertions, and test cases are divided into different *profiles.*

4.1.1 Profiles

Listed below are profiles included for the sake of organized distinction.

- **Image file artifacts**

  Different types of mobile artifacts are included in this profile. These artifacts are deduced from subscriber information, call data, message data, media files, browsing data, email data, and application data. Most of the requirements, test assertions, and test cases are related to this profile.

- **Image File acquisition**

  Details about image acquisition whether physical or logical encompass this profile.

- **UICC acquisition**

  A UICC is a removable module that contains various details about the subscriber, this profile encompasses all the artifacts related to the UICC module.

- **Deleted data artifacts**

  Recoverable deleted data artifacts are included in this profile.

- **SQLite database**

This profile includes various kinds of features of an SQLLITE database to check whether a mobile forensic tool provides the SQLLITE database with all the features for the ease of a forensic investigator.

4.2 Requirements for Mobile Forensics Tools

The requirements provided in the mobile device test specification document by CFTT are divided into core and optional requirements. Following is the terminology used by the standard CFTT nomenclature:

- MDT–Mobile Device Tool
- CR–Core Requirement
- OR–Optional Requirement
- CA– Core Assertion
- AO– Optional Assertion

For example, MDT-CR-01 refers to the first core requirement for the mobile forensics tool.

4.2.1 Core Requirements

The core requirements are mandatory for a tool and CFTT provides four core requirements for mobile forensic tools. The core requirements cover the first profile, i.e. image file artifacts.

4.2.2 Optional Requirements

The optional requirements are non-mandatory for the tool and twelve of them are provided by the CFTT documentation. They cover the rest of the four profiles namely image file acquisition, UICC acquisition, deleted data artifacts. and SQLLITE database.

4.3 Proposed Extended CFTT-based Framework

The following figure represents the overall proposed framework.

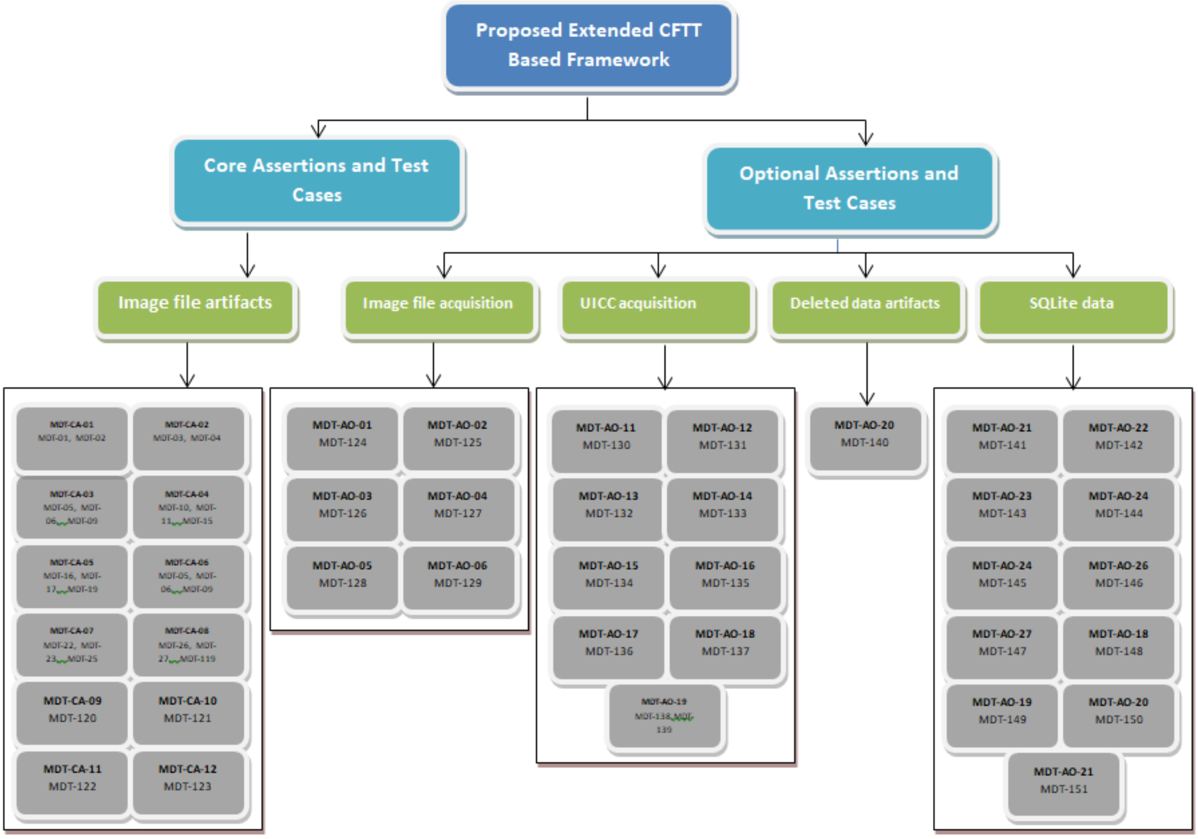


Fig 4.1 Proposed Extended CFTT based Framework

The test assertions from the CFTT document and the derived test cases are laid down below. They map to the core and optional requirements provided in the CFTT document.

4.3.1 Core Assertions and Test Cases

4.3.1.1 Image file artifacts

MDT-CA-01: The tool presents all subscriber and equipment information available from an image file.		
Proposed Test Actions	*MDT-01:*	Attempt to view subscriber information
	MDT-02:	Attempt to view equipment information
Conformance Indicator: The digital forensics tool determined subscriber and equipment		

information.

Table 4.1 Subscriber and equipment information

MDT-CA-02: The tool presents all PIM (address book, calendar & notes) data available from an image file		
Proposed Test Actions	*MDT-03:*	Attempt to view address book data.
	MDT-04:	Attempt to view calendar & notes.
Conformance Indicator: The digital forensics tool presented all PIM data.		

Table 4.2 PIM data

MDT-CA-03: The tool presents all call data (call type (incoming, outgoing, missed), datetime stamps, duration) available from an image file.		
Proposed Test Actions	*MDT-05:*	Attempt to view incoming call data.
	MDT-06:	Attempt to view outgoing call data.
	MDT-07:	Attempt to view missed call data.
	MDT-08:	Attempt to view timetamps.
	MDT-09:	Attempt to view duration of calls.
Conformance Indicator: The digital forensics tool presented all call data.		

Table 4.3 Call data

MDT-CA-04: The tool presents all message (SMS, MMS & instant messages) data available from an image file.		
Proposed Test Actions	*MDT-10:*	Attempt to view local messages.
	MDT-11:	Attempt to view MMS messages.
	MDT-12:	Attempt to view instant messages.
	MDT-13:	Attempt to view local messages’ timestamps.

	MDT-14:	Attempt to view MMS messages’ timestamps.
	MDT-15:	Attempt to view instant messages’ timestamps.
Conformance Indicator: The digital forensics tool presented all message data.		

Table 4.4 Message data

MDT-CA-05: The tool presents all stand-alone (audio, documents, graphic & video,) files available from an image file.		
Proposed Test Actions	*MDT-16:*	Attempt to view audio files
	MDT-17:	Attempt to view videos.
	MDT-18:	Attempt to view documents.
	MDT-19:	Attempt to view image files.
Conformance Indicator: The digital forensics tool presented the stand-alone files.		

Table 4.5 Stand-alone files

MDT-CA-06: The tool presents all browsing (history & bookmarks) data available from an image file.		
Proposed Test Actions	*MDT-20:*	Attempt to view history.
	MDT-21:	Attempt to view bookmarks.
Conformance Indicator: The digital forensics tool presented browsing data.		

Table 4.6 Browsing history

MDT-CA-07: The tool presents all email data available from an image file.		
Proposed Test Actions	*MDT-22:*	Attempt to search for the sender of an email.
	MDT-23:	Attempt to search for the receiver of an email.
	MDT-24:	Attempt to search for the content of an email.
	MDT-25:	Attempt to search for the timestamp of an email.

Conformance Indicator: The digital forensics tool presented all the email data.

Table 4.7 Email data

MDT-CA-08: The tool presents all social media application data available from an image file.		
Proposed Social Media Application Test Actions	*MDT-26:*	Attempt to view the contact name from the social media application database.
	MDT-27:	Attempt to view contact profile image from the social media application database.
	MDT-28:	Attempt to view a contact's phone number from the social media application database.
	MDT-29:	Attempt to view blocked contact profile image from the social media application database.
	MDT-30:	Attempt to view a blocked contact's phone number from the social media application database.
	MDT-31:	Attempt to view the phone number of a sender of a chat message from the social media application database.
	MDT-32:	Attempt to view the phone number of a receiver of a chat message from the social media application database.
	MDT-33:	Attempt to view time stamp of a chat message from the social media application database.
	MDT-34:	Attempt to view chat content of a chat message from the social media application database.
	MDT-35:	Attempt to view the phone number of a sender of a forwarded message from the social media application database.
	MDT-36:	Attempt to view the phone number of a receiver of a forwarded message from the social media application database.
	MDT-37:	Attempt to view time stamp of a forwarded message from the social media application database.

	MDT-38:	Attempt to view chat content of a forwarded message from the social media application database.
	MDT-39:	Attempt to view original author of a forwarded message from the social media application database.
	MDT-40:	Attempt to view the phone number of a sender of a starred message from the social media application database.
	MDT-41:	Attempt to view the phone number of a receiver of a starred message from the social media application database.
	MDT-42:	Attempt to view the time stamp of a starred message from the social media application database.
	MDT-43:	Attempt to view the chat content of a starred message from the social media application database.
	MDT-44:	Attempt to view the phone number of a sender of a disappearing message from the social media application database.
	MDT-45:	Attempt to view the phone number of a receiver of a disappearing message from the social media application database.
	MDT-46:	Attempt to view the time stamp of a disappearing message from the social media application database.
	MDT-47:	Attempt to view the chat content of a disappearing message from the social media application database.
	MDT-48:	Attempt to view the duration of a disappearing message from the social media application database.
	MDT-49:	Attempt to view a disappearing message after it has disappeared from the social media application database.
	MDT-50:	Attempt to view the phone number of a sender of a voice message from the social media application database.
	MDT-51:	Attempt to view the phone number of a receiver of a voice message from the social media application

		database.
	MDT-52:	Attempt to view the time stamp of a voice message from the social media application database.
	MDT-53:	Attempt to view the chat content of a voice message from the social media application database.
	MDT-54:	Attempt to view the phone number of a caller of a voice call from the social media application database.
	MDT-55:	Attempt to view the phone number of a receiver of a voice call from the social media application database.
	MDT-56:	Attempt to view the time stamp of a voice call from the social media application database.
	MDT-57:	Attempt to view the duration of a voice call from the social media application database.
	MDT-58:	Attempt to view the phone number of a caller of a video call from the social media application database.
	MDT-59:	Attempt to view the phone number of a receiver of a video call from the social media application database.
	MDT-60:	Attempt to view the time stamp of a video call from the social media application database.
	MDT-61:	Attempt to view the duration of a video call from the social media application database.
	MDT-62:	Attempt to view the phone number of a sender of a media file from the social media application database.
	MDT-63:	Attempt to view the phone number of a receiver of a media file from the social media application database.
	MDT-64:	Attempt to view the content of a media file from the social media application database.
	MDT-65:	Attempt to view the type of a media file from the social media application database.
	MDT-66:	Attempt to view the uploader’s phone number of an uploaded status from the social media application database.

	MDT-67:	Attempt to view the timestamp of an uploaded status from the social media application database.
	MDT-68:	Attempt to view the type of an uploaded status from the social media application database.
	MDT-69:	Attempt to view the content of an uploaded status from the social media application database.
	MDT-70:	Attempt to view the viewers of an uploaded status from the social media application database.
	MDT-71:	Attempt to view the timestamp of an uploaded status after 24 hours from the social media application database.
	MDT-72:	Attempt to view the type of an uploaded status after 24 hours from the social media application database.
	MDT-73:	Attempt to view the content of an uploaded status after 24 hours from the social media application database.
	MDT-74:	Attempt to view the viewers of an uploaded status after 24 hours from the social media application database.
	MDT-75:	Attempt to view the time when a group was created from the social media application database.
	MDT-76:	Attempt to view the admin of a group from the social media application database.
	MDT-77:	Attempt to the view phone number of a group's participant from the social media application database.
	MDT-78:	Attempt to view the phone number of a sender of a chat message in a group a from the social media application database.
	MDT-79:	Attempt to view the time stamp of a group's chat message from the social media application database.
	MDT-80:	Attempt to view the content of a group's chat message from the social media application database.
	MDT-81:	Attempt to view the phone number of a sender of a disappearing message in a group a from the social media application database.

	MDT-82:	Attempt to view the time stamp of a group’s disappearing message from the social media application database.
	MDT-83:	Attempt to view the content of a group’s disappearing message from the social media application database.
	MDT-84:	Attempt to view the duration of a group’s disappearing message from the social media application database.
	MDT-85:	Attempt to view the content of a group’s disappearing message after it has disappeared from the social media application database.
	MDT-86:	Attempt to view the the phone number of a sender of a voice message in a group a from the social media application database.
	MDT-87:	Attempt to view the time stamp of a group’s voice message from the social media application database.
	MDT-88:	Attempt to the view content of a group’s voice message from the social media application database.
	MDT-89:	Attempt to view the phone number of a caller of the group voice call in a group a from the social media application database.
	MDT-90:	Attempt to view the phone number of participants of the group voice call in a group a from the social media application database.
	MDT-91:	Attempt to view the time stamp of a group voice call from the social media application database.
	MDT-92:	Attempt to view the duration of a group voice call from the social media application database.
	MDT-93:	Attempt to viewthe phone number of a group video call in a group a from the social media application database.
	MDT-94:	Attempt to view the phone number of the participants of the group video call in a group a from the social media application database.
	MDT-95:	Attempt to view the time stamp of a group video call

		from the social media application database.
	MDT-96:	Attempt to view the duration of a group video call from the social media application database.
	MDT-97:	Attempt to view the phone number of a sender of a media file in a group from the social media application database.
	MDT-98:	Attempt to view the timestamp sent of a media file in a group from the social media application database.
	MDT-99:	Attempt to view the type of a media file sent in a group from the social media application database.
	MDT-100:	Attempt to view the content of a media file sent in a group from the social media application database.
	MDT-101:	Attempt to view the time when a broadcast was created from the social media application database.
	MDT-102:	Attempt to view the phone number of a broadcast's creator from the social media application database.
	MDT-103:	Attempt to view the phone number of a broadcast's recipient from the social media application database.
	MDT-104:	Attempt to view the time stamp of a broadcasted chat message from the social media application database.
	MDT-105:	Attempt to view the content of a broadcasted chat message from the social media application database.
	MDT-106:	Attempt to view the time stamp of a broadcasted voice message from the social media application database.
	MDT-107:	Attempt to the view content of a broadcasted voice message from the social media application database.
	MDT-108:	Attempt to the view time stamp of a broadcasted media file from the social media application database.
	MDT-109:	Attempt to view the type of a broadcasted media file from the social media application database.
	MDT-110:	Attempt to view the content of a broadcasted media file from the social media application database.

	MDT-111:	Attempt to view the phone number of the sender of a secret message from the social media application database.
	MDT-112:	Attempt to view the phone number of a receiver of a secret message from the social media application database.
	MDT-113:	Attempt to view the time stamp of a secret message from the social media application database.
	MDT-114:	Attempt to view the chat content of a secret message from the social media application database.
	MDT-115:	Attempt to view the phone number of a sender of an edited message from the social media application database.
	MDT-116:	Attempt to view the phone number of a receiver of an edited message from the social media application database.
	MDT-117:	Attempt to view the time stamp when a message was edited from the social media application database.
	MDT-118:	Attempt to view the chat content of an edited message from the social media application database.
	MDT-119:	Attempt to view the edit history of an edited message from the social media application database.
Conformance Indicator: The digital forensics tool presented all social media application data.		

Table 4.8 Social media application data

MDT-CA-09: The tool presents all geo-location application data available from an image file.		
Proposed Test Actions	*MDT-120:*	Attempt to search for location coordinates present in the database of the application.
Conformance Indicator: The digital forensics tool presented all geo-location application data.		

Table 4.9 Geo-Location application data

MDT-CA-10: Presented text is rendered with the correct character glyphs.		
Proposed Test Actions	*MDT-121:*	Attempt to view text presented from the image file analyzed by the tool.
Conformance Indicator: The digital forensics tool presented the text with the correct character glyphs.		

Table 4.10 Character glyphs

MDT-CA-11: The tool does not modify an image file		
Proposed Test Actions	*MDT-122:*	Compare the data of an image file with the original data.
Conformance Indicator: The digital forensics tool made no changes to the image file.		

Table 4.11 Image file modification

MDT-CA-12: If an image file is modified, the tool notifies the user that a change has been made to the image file.		
Proposed Test Actions	*MDT-123:*	Attempt to modify the image file.
Conformance Indicator: The digital forensics tool notified the user of image file modification.		

Table 4.12 Image file modification notification

4.3.2 Optional Assertions and Test Cases

4.3.2.1 Image file acquisition

MDT-AO-01: An image file is created of physical memory.		
Proposed Test Actions	*MDT-124:*	Attempt to create an image of physical memory.
Conformance Indicator: The digital forensics tool created a physical memory image successfully.		

Table 4.13 Physical memory image file

MDT-AO-02: An image file is created containing supported memory artifacts.		
Proposed Test Actions	*MDT-125:*	Attempt to create a logical image of the mobile device.
Conformance Indicator: The digital forensics tool created a logical image successfully.		

Table 4.14 Supported memory artifacts image file

MDT-AO-03: An image file is created containing selected artifacts.		
Proposed Test Actions	*MDT-126:*	Attempt to create an image file of selected artifacts.
Conformance Indicator: The digital forensics tool created an image file of selected artifacts successfully.		

Table 4.15 Selected artifacts image file

MDT-AO-04: An image file is created of the device file system.		
Proposed Test Actions	*MDT-127:*	Attempt to create an image file of the file system.
Conformance Indicator: The digital forensics tool created an image file of the file system successfully.		

Table 4.16 Device file system image file

MDT-AO-05: The user is notified if the tool fails to establish a connection or acquire data from a connected mobile device.		
Proposed Test Actions	*MDT-128:*	Attempt to acquire an image.
Conformance Indicator: The digital forensics tool notified the user in case of failure during image acquisition.		

Table 4.17 Failed acquisition notification

MDT-AO-06: The user is notified if an acquisition is disrupted		
Proposed Test Actions	*MDT-129:*	Disconnect the device during acquisition.
Conformance Indicator: The digital forensics tool notified the user in case of disruption during image acquisition.		

Table 4.18 Interrupted acquisition notification

4.3.2.2 UICC acquisition

MDT-AO-11: An image file is created containing supported UICC artifacts.		
Proposed Test Actions	*MDT-130:*	Create an image file.
Conformance Indicator: The digital forensics tool successfully created an image file containing UICC artifacts.		

Table 4.19 UICC image file creation

MDT-AO-12: A mobile device forensic tool presents Service Provider Name (SPN) from a UICC image file		
Proposed Test Actions	*MDT-131:*	Search for SPN from the UICC image file.
Conformance Indicator: The digital forensics tool successfully presented the SPN from the UICC image file.		

Table 4.20 SPN Detection

MDT-AO-13: A mobile device forensic tool presents Integrated Circuit Card Identifier (ICCID) from a UICC image file.		
Proposed Test Actions	*MDT-132:*	Search for ICCID from the UICC image file.
Conformance Indicator: The digital forensics tool successfully presented the ICCID from the UICC image file.		

Table 4.21 ICCID Detection

<table>
<tr><td colspan="3"><b>MDT-AO-14:</b> A mobile device forensic tool presents International Mobile Subscriber Identity (IMSI) from a UICC image file.</td></tr>
<tr><td><b>Proposed Test Actions</b></td><td><i>MDT-133:</i></td><td>Search for IMSI from the UICC image file.</td></tr>
<tr><td colspan="3">Conformance Indicator: The digital forensics tool successfully presented the IMSI from the UICC image file.</td></tr>
</table>

Table 4.22 IMSI Detection

<table>
<tr><td colspan="3"><b>MDT-AO-15:</b> A mobile device forensic tool presents Mobile Subscriber International ISDN Number (MSISDN) from a UICC image file.</td></tr>
<tr><td><b>Proposed Test Actions</b></td><td><i>MDT-134:</i></td><td>Search for MSISDN from the UICC image file.</td></tr>
<tr><td colspan="3">Conformance Indicator: The digital forensics tool successfully presented the MSISDN from the UICC image file.</td></tr>
</table>

Table 4.23 MSISDN Detection

<table>
<tr><td colspan="3"><b>MDT-AO-16:</b> A mobile device forensic tool presents Abbreviated Dialing Numbers (ADNs) from a UICC image file.</td></tr>
<tr><td><b>Proposed Test Actions</b></td><td><i>MDT-135:</i></td><td>Search for ADNs from the UICC image file.</td></tr>
<tr><td colspan="3">Conformance Indicator: The digital forensics tool successfully presented the ADNs from the UICC image file.</td></tr>
</table>

Table 4.24 ADNs Detection

<table>
<tr><td colspan="3"><b>MDT-AO-17:</b> A mobile device forensic tool presents Last Numbers Dialed (LND) from a UICC image file.</td></tr>
<tr><td><b>Proposed Test Actions</b></td><td><i>MDT-136:</i></td><td>Search for LND from the UICC image file.</td></tr>
<tr><td colspan="3">Conformance Indicator: The digital forensics tool successfully presented the LDN from the</td></tr>
</table>

UICC image file.

Table 4.25 LND Detection

MDT-AO-18: A mobile device forensic tool presents Text messages (SMS) from a UICC image file.		
Proposed Test Actions	*MDT-137:*	Attempt to view SMS messages.
Conformance Indicator: The digital forensics tool successfully presented SMS messages from the UICC image file.		

Table 4.26 SMS Detection

MDT-AO-19: A mobile device forensic tool presents Location (LOCI, GPRSLOCI) from a UICC image file.		
Proposed Test Actions	*MDT-138:*	Attempt to view LOCI.
	MDT-139:	Attempt to view GPRSLOCI.
Conformance Indicator: The digital forensics tool successfully presented the Location from the UICC image file.		

Table 4.27 Location identification

4.3.2.3 Deleted data artifacts

MDT-AO-20: If an image file contains recoverable deleted data artifacts and the tool supports data recovery, then the tool presents the recovered deleted items.		
Proposed Test Actions	*MDT-140:*	Search deleted data artifacts from the image.
Conformance Indicator: The digital forensics tool successfully presented deleted data items.		

Table 4.28 Deleted artifacts recovery

4.3.2.4 SQLite data

MDT-AO-21: The tool shall display numeric values.		
Proposed Test Actions	*MDT-141:*	Attempt to view numeric value from image file.
Conformance Indicator: The digital forensics tool successfully presented numeric value.		

Table 4.29 Numeric values

MDT-AO-22: The tool shall display integer time values as a conventional human readable date and time.		
Proposed Test Actions	*MDT-142:*	Attempt to view the date and time from an image file.
Conformance Indicator: The digital forensics tool presented date and time in human-readable form.		

Table 4.30 Integer values

MDT-AO-23: The tool shall render text for Text fields, table names, and column names encoded in Unicode Transformation Format (UTF) 8, UTF 16BE, and UTF 16LE.		
Proposed Test Actions	*MDT-143:*	Attempt to view UTF-encoded data.
Conformance Indicator: The digital forensics tool rendered data encoded in UTF.		

Table 4.31 Render UTF-encoded data

MDT-AO-24: The tool shall decode and display base64 encoded text.		
Proposed Test Actions	*MDT-144:*	Attempt to view base64 encoded text from an image file.
Conformance Indicator: The digital forensics tool successfully decoded and displayed base64 text.		

Table 4.32 base64 encoded data

MDT-AO-25: The tool shall display graphic image data recorded as a BLOB in the

database.		
Proposed Test Actions	*MDT-145:*	Attempt to view the image recorded as BLOB.
Conformance Indicator: The digital forensics tool successfully displayed the image recorded as BLOB.		

Table 4.33 BLOB image data

MDT-AO-26: The tool shall decode data recorded as a BLOB in the database.		
Proposed Test Actions	*MDT-146:*	Attempt to view data recorded as BLOB.
Conformance Indicator: The digital forensics tool successfully displayed the data recorded as BLOB.		

Table 4.34 BLOB data

MDT-AO-27: The tool shall have the ability to display SQLite BLOB data (e.g., graphic files and plist).		
Proposed Test Actions	*MDT-147:*	Attempt to view SQLite BLOB data from the image file.
Conformance Indicator: The digital forensics tool successfully displayed the SQLite BLOB data		

Table 4.35 SQLite BLOB data

MDT-AO-28: The tool shall report all currently active data when WAL mode is in use.		
Proposed Test Actions	*MDT-148:*	Attempt to view data in WAL mode.
Conformance Indicator: The digital forensics tool successfully presented live data in WAL mode.		

Table 4.36 View data in WAL mode

MDT-AO-29: The tool shall report all currently active data when journal mode is in use.		
Proposed Test Actions	*MDT-149:*	Attempt to view data in journal mode.
Conformance Indicator: The digital forensics tool successfully presented live data in WAL mode.		

Table 4.37 View data in journal mode

MDT-AO-30: The tool shall execute SQLite commands and report the results.		
Proposed Test Actions	*MDT-150:*	Attempt to execute SQLite commands.
Conformance Indicator: The digital forensics tool successfully executed SQLite commands and reported the results.		

Table 4.38 SQLite commands execution

MDT-AO-31: The tool shall have the ability to save SQLite commands for later recall.		
Proposed Test Actions	*MDT-151:*	Attempt to save SQLite commands.
Conformance Indicator: The digital forensics tool successfully saved SQLite commands.		

Table 4.39 Saving SQLite commands

A summary of the entire evaluation framework is provided in Table 4.40 and 4.41 as follows.

Profiles	**Core Requirements**	**Core Assertions**	**Proposed Test-Cases**
Image file artifacts	MDT-CR-01	MDT -CA-01 MDT -CA-02 MDT -CA-03 MDT -CA-04 MDT -CA-05 MDT -CA-06 MDT -CA-07 MDT -CA-08 MDT -CA-09	MDT-01, MDT-02 MDT-03, MDT-04 MDT-05, MDT-06, … MDT-09 MDT-10, MDT-11, … MDT-15 MDT-16, MDT-17, … MDT-19 MDT-20, MDT-21 MDT-22, MDT-23, … MDT-25 MDT-26, MDT-27, … MDT-119 MDT-120
	MDT-CR-02 MDT-CR-03 MDT-CR-04	MDT -CA-10 MDT -CA-11 MDT -CA-12	MDT-121 MDT-122 MDT-123

Table 4.40– The Digital Forensics Tools Evaluation Criteria (Core)

Profiles	Optional Requirements	Optional Assertions	Proposed Test-Cases
Image file acquisition	MDT-RO-01 MDT-RO-02 MDT-RO-03 MDT-RO-04 MDT-RO-05 MDT-RO-06	MDT-AO-01 MDT-AO-02 MDT-AO-03 MDT-AO-04 MDT-AO-05 MDT-AO-06	MDT-124 MDT-125 MDT-126 MDT-127 MDT-128 MDT-129
UICC Acquisition	MDT-RO-08	MDT-AO-11	MDT-130
	MDT-RO-09	MDT-AO-12 MDT-AO-13 MDT-AO-14 MDT-AO-15 MDT-AO-16 MDT-AO-17 MDT-AO-18 MDT-AO-19	MDT-131 MDT-132 MDT-133 MDT-134 MDT-135 MDT-136 MDT-137 MDT-138,MDT-139
Deleted data artifacts	MDT-RO-10	MDT-AO-20	MDT-140
SQLite database	MDT-RO-11 MDT-RO-12	MDT-AO-21 MDT-AO-22 MDT-AO-23 MDT-AO-24 MDT-AO-25 MDT-AO-26 MDT-AO-27 MDT-AO-28 MDT-AO-29 MDT-AO-30 MDT-AO-31	MDT-141 MDT-142 MDT-143 MDT-144 MDT-145 MDT-146 MDT-147 MDT-148 MDT-149 MDT-150 MDT-151

Table 4.41– The Digital Forensics Tools Evaluation Criteria (Optional)

Most of the test cases were derived from the core test assertions that came under the “Image file artifacts” profile, i.e., 123 test cases. The rest of the test cases were derived from optional assertions. From the “Image file acquisition” profile, 6 test cases were derived. From the “UICC acquisition” profile, 10 test cases were derived. One test case was derived from the “deleted data artifacts” profile and 11 test cases were derived from the “SQLite database” profile.

4.4 Summary

This chapter explained the profiles encompassing CFTT test requirements, test assertions, and test cases. CFTT nomenclature was also mentioned in this chapter. Later the proposed test cases derived from CFTT test assertions were presented and summarised in table format against the CFTT profiles and test requirements.

5. Experimental Results

At the beginning of this chapter, a feature list of forensic tools is provided. Next, the working environment is presented under which the test cases were performed for each tool. This is followed by the forensic tool specification. After this, the experimental analysis of forensic tools was explained that how a test case is performed on a forensic tool and how the results are displayed. Next, the detailed test results are provided. These test results are then tabulated comparatively. This chapter is summarized at the end.

5.1 Feature Lists

To test the three mobile forensic tools, proposed framework, three mobile forensics tools were tested namely Autopsy, Andriller, and AFLogical.

Table 5.1 lists the features of each tool.

Features	Autopsy	Andriller	AFLogical
Open-source Tool	✔	✔	✔
Non-commercial Tool	✔	✔	✔
Physical image extraction	✔	✖	✖
Logical Image Extraction	✔	✔	✔
Selected files analysis	✔	✖	✖
SQLite database	✔	✖	✖

Table5.1–List of Tools with its Features

5.2 Working Environment and Forensic Tool Specification

5.2.1 Execution Environment

Execution Environment: Windows 10

Processor: Intel(R)Core (TM)i7-6820CPU@2.70GHz

Installed Memory(RAM):	32.0 GB
System Type:	x64-basedPC
Test Computer:	HP ZBook Studio G3
Test Device 1: Samsung	Galaxy Grand Prime
Android Version:	5.0.2
Test Device 2:	OPPO F9
Android Version:	10.0.0

5.2.2 Forensic Tools Specification

Forensic tool	Description	Software Version	Supplier	Website
Autopsy	Autopsy is an open-source and non-commercial digital forensic software. It can be accessed using Windows, Linux and, OS X.	4.20.0	Basis Technology	https://www.sleuthkit.org/autopsy/
Andriller	Andriller is an open-source mobile forensic software. It can be run on Windows.	3.5.3	Denis Sazonov	https://github.com/den4uk/andriller
AFLogical	AFLogical is an open-source Android forensic application that extracts logical data from Android phones.	1.5.2	Tom Anderson	https://github.com/nowsecure/android-forensics

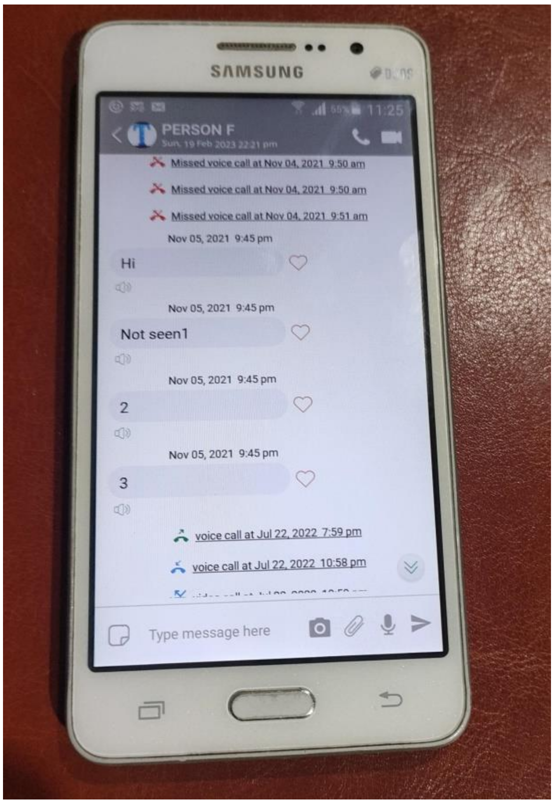
Table 5.2– Forensic Tools Specification

5.2.3 Forensic Tools Experimental analysis:

Experiments were conducted by performing different user activities on the mobile phone. Test cases related to offline mobile phone data were conducted by performing user activities related to offline mobile activities like calling, messaging, making calendar events, writing notes, and creating and storing different kinds of media files. Test cases related to social media application data were executed by performing the user activities for each social media application feature.

Following is an evaluation of test cases from MDT-31 to MDT-33, in which the Autopsy forensic tool is supposed to identify the identity of the sender and receiver (MDT-31 and MDT-32) and content (MDT-33) of a chat message sent in KalamTime application.

The following screenshot presents the user activity of sending a chat message from the test device to another user device.



PERSON F
Sun, 19 Feb 2023 22:21 pm

Missed voice call at Nov 04, 2021 9:50 am
Missed voice call at Nov 04, 2021 9:50 am
Missed voice call at Nov 04, 2021 9:51 am

Nov 05, 2021 9:45 pm
Hi

Nov 05, 2021 9:45 pm
Not seen1

Nov 05, 2021 9:45 pm
2

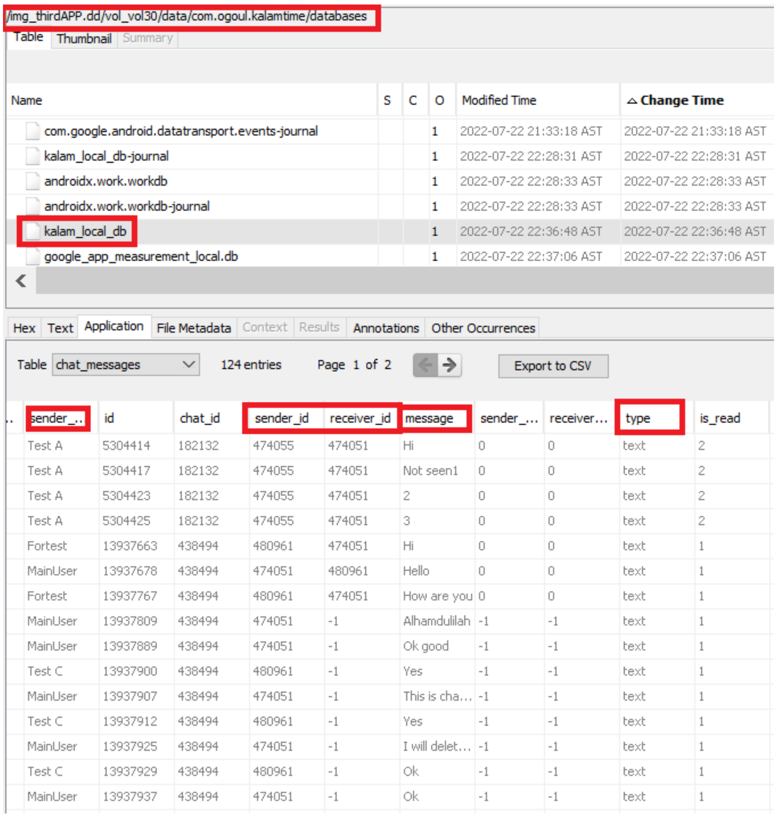
Nov 05, 2021 9:45 pm
3

voice call at Jul 22, 2022 7:59 pm
voice call at Jul 22, 2022 10:58 pm

Fig 5.1 User Activity on the Test Device

Following are the test results obtained from analysis of Autopsy Forensic tool.

Test case id	MDT-31, MDT-32, MDT-33
Test case result	As expected
Test case analysis	Autopsy successfully displayed a chat message’s sender, receiver, timestamp, and content in the KalamTime app.

Screenshots	

/img_thirdAPP.dd/vol_vol30/data/com.ogoul.kalamtime/databases

Name	S	C	O	Modified Time	Change Time
com.google.android.datatransport.events-journal			1	2022-07-22 21:33:18 AST	2022-07-22 21:33:18 AST
kalam_local_db-journal			1	2022-07-22 22:28:31 AST	2022-07-22 22:28:31 AST
androidx.work.workdb			1	2022-07-22 22:28:33 AST	2022-07-22 22:28:33 AST
androidx.work.workdb-journal			1	2022-07-22 22:28:33 AST	2022-07-22 22:28:33 AST
kalam_local_db			1	2022-07-22 22:36:48 AST	2022-07-22 22:36:48 AST
google_app_measurement_local.db			1	2022-07-22 22:37:06 AST	2022-07-22 22:37:06 AST

Table chat_messages 124 entries Page 1 of 2

sender_...	id	chat_id	sender_id	receiver_id	message	sender_...	receiver...	type	is_read
Test A	5304414	182132	474055	474051	Hi	0	0	text	2
Test A	5304417	182132	474055	474051	Not seen1	0	0	text	2
Test A	5304423	182132	474055	474051	2	0	0	text	2
Test A	5304425	182132	474055	474051	3	0	0	text	2
Fortest	13937663	438494	480961	474051	Hi	0	0	text	1
MainUser	13937678	438494	474051	480961	Hello	0	0	text	1
Fortest	13937767	438494	480961	474051	How are you	0	0	text	1
MainUser	13937809	438494	474051	-1	Alhamdulilah	-1	-1	text	1
MainUser	13937889	438494	474051	-1	Ok good	-1	-1	text	1
Test C	13937900	438494	480961	-1	Yes	-1	-1	text	1
MainUser	13937907	438494	474051	-1	This is cha...	-1	-1	text	1
Test C	13937912	438494	480961	-1	Yes	-1	-1	text	1
MainUser	13937925	438494	474051	-1	I will delet...	-1	-1	text	1
Test C	13937929	438494	480961	-1	Ok	-1	-1	text	1
MainUser	13937937	438494	474051	-1	Ok	-1	-1	text	1

Table 5.3– Experimental Analysis

As the Autopsy Forensic tool successfully confirmed the test cases, they were marked "As expected" in the test results.

5.3 Detailed Test Results

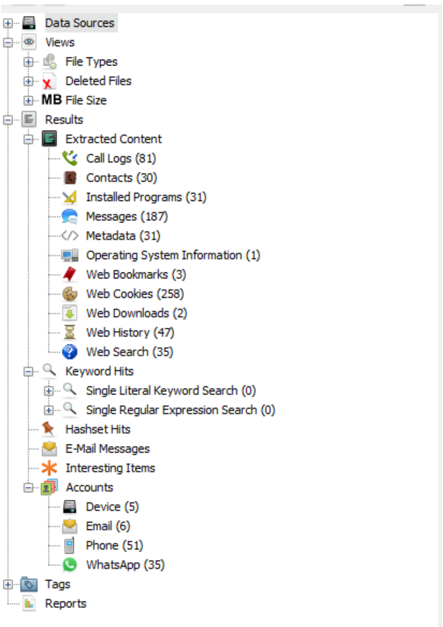
This section provides details of the test results of each of the three tools. The results are presented with respect to test case IDs. Each test case is tested and the results are listed in the respective table. The possible result values in the table are explained below:

1. **As expected** means the tool successfully conformed to the test case (this map to 1 in Table 5.87(a), 5.87(b), and 5.87(c)).
2. **Not checked** means the tool was unable to conform to the test case (this map to 0 in Table 5.87(a), 5.87(b), and 5.87(c)).

3. **Option not available** means the tool does not provide the feature (this maps to N/A in Table 5.87(a), 5.87(b), and 5.87(c))

4. **Successful in combination with another tool** means the tool successfully conformed to the test case but in combination with another tool (this maps to 2 in Table 5.87(a),5.87(b), and 5.87(c)

5.3.1 Autopsy Test Results Report



- Data Sources
- Views
  - File Types
  - Deleted Files
  - MB File Size
- Results
  - Extracted Content
    - Call Logs (81)
    - Contacts (30)
    - Installed Programs (31)
    - Messages (187)
    - Metadata (31)
    - Operating System Information (1)
    - Web Bookmarks (3)
    - Web Cookies (258)
    - Web Downloads (2)
    - Web History (47)
    - Web Search (35)
  - Keyword Hits
    - Single Literal Keyword Search (0)
    - Single Regular Expression Search (0)
  - Hashset Hits
  - E-Mail Messages
  - Interesting Items
  - Accounts
    - Device (5)
    - Email (6)
    - Phone (51)
    - WhatsApp (35)
- Tags
- Reports

Fig 5.2 Autopsy Overall Extraction Results

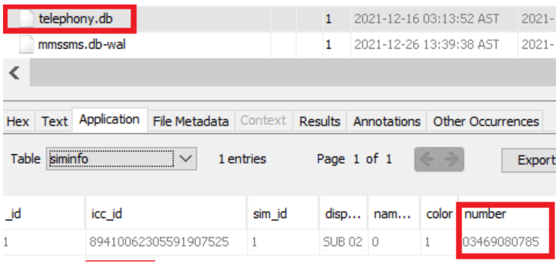
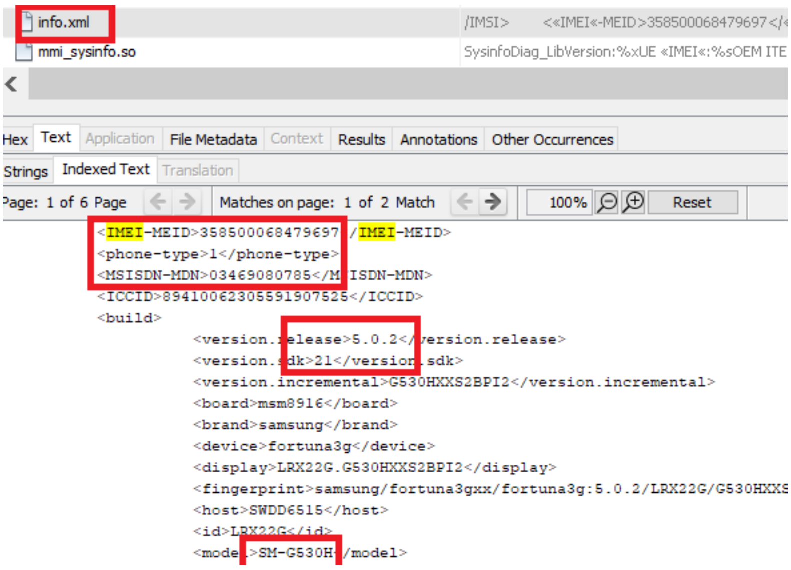
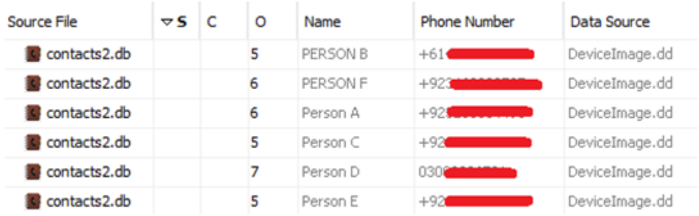
Test case id	MDT-01
Test case result	As expected
Test case analysis	Autopsy was able to show the subscriber’s information.
Screenshots	 telephony.db 1 2021-12-16 03:13:52 AST 2021- mmssms.db-wal 1 2021-12-26 13:39:38 AST 2021- Hex Text Application File Metadata Context Results Annotations Other Occurrences Table siminfo 1 entries Page 1 of 1 Export _id icc_id sim_id disp... nam... color number 1 89410062305591907525 1 SUB 02 0 1 03469080785

Table 5.4–Autopsy Test Result MDT-01

Test case id	MDT-02
Test case result	As expected
Test case analysis	Autopsy was able to show the equipment information.
Screenshots	

```
<IMEI-MEID>358500068479697</IMEI-MEID>
<phone-type>1</phone-type>
<MSISDN-MDN>03469080785</MSISDN-MDN>
<ICCID>89410062305591907525</ICCID>
<build>
            <version.release>5.0.2</version.release>
            <version.sdk>21</version.sdk>
            <version.incremental>G530HXXS2BPI2</version.incremental>
            <board>msm8916</board>
            <brand>samsung</brand>
            <device>fortuna3g</device>
            <display>LRX22G.G530HXXS2BPI2</display>
            <fingerprint>samsung/fortuna3gxx/fortuna3g:5.0.2/LRX22G/G530HXXS
            <host>SWDD6515</host>
            <id>LRX22G</id>
            <model>SM-G530H</model>
```

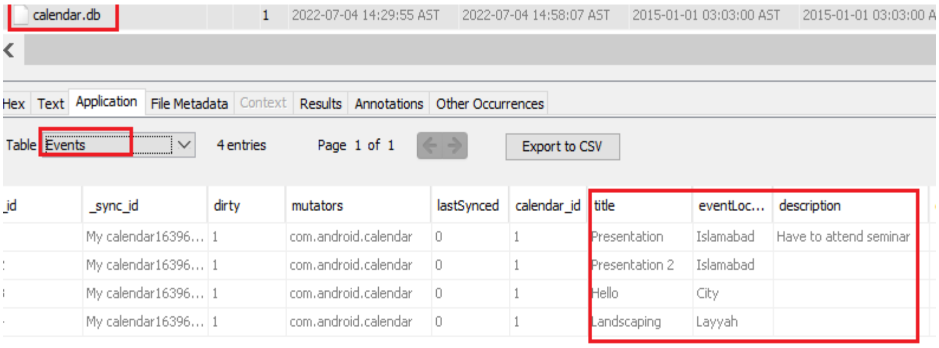
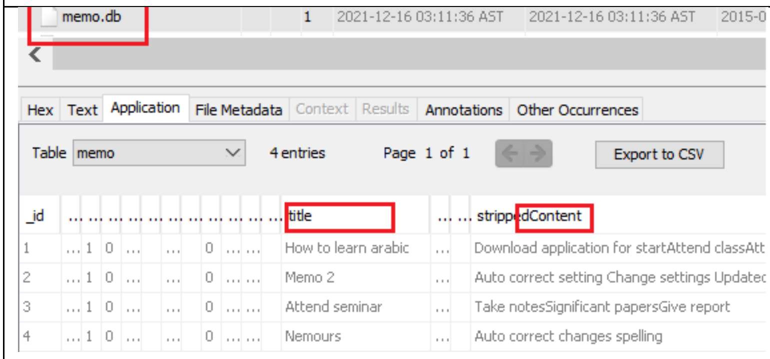
Table 5.5– Autopsy Test Result MDT-02

Test case id	MDT-03
Test case result	As expected
Test case analysis	Autopsy was able to show the address book data.
Screenshots	

Source File	S	C	O	Name	Phone Number	Data Source
contacts2.db			5	PERSON B	+61[redacted]	DeviceImage.dd
contacts2.db			6	PERSON F	+923[redacted]	DeviceImage.dd
contacts2.db			6	Person A	+92[redacted]	DeviceImage.dd
contacts2.db			5	Person C	+92[redacted]	DeviceImage.dd
contacts2.db			7	Person D	030[redacted]	DeviceImage.dd
contacts2.db			5	Person E	+92[redacted]	DeviceImage.dd

Table 5.6– Autopsy Test Result MDT-03

Test case id	MDT-04

Test case result	As expected
Test case analysis	Autopsy was able to show the calendar and notes' information.
Screenshots	 

calendar.db 1 2022-07-04 14:29:55 AST 2022-07-04 14:58:07 AST 2015-01-01 03:03:00 AST 2015-01-01 03:03:00 A

Table Events 4 entries Page 1 of 1

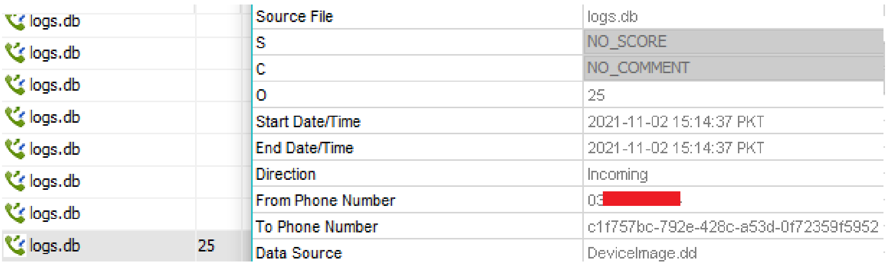
_id	_sync_id	dirty	mutators	lastSynced	calendar_id	title	eventLoc...	description
	My calendar16396...	1	com.android.calendar	0	1	Presentation	Islamabad	Have to attend seminar
	My calendar16396...	1	com.android.calendar	0	1	Presentation 2	Islamabad	
	My calendar16396...	1	com.android.calendar	0	1	Hello	City	
	My calendar16396...	1	com.android.calendar	0	1	Landscaping	Layyah	

memo.db 1 2021-12-16 03:11:36 AST 2021-12-16 03:11:36 AST 2015-0

Table memo 4 entries Page 1 of 1

_id	...	...	...	...	...	...	...	...	...	...	...	title	...	...	strippedContent
1	...	1	0	...		...		0	...	...		How to learn arabic	...		Download application for startAttend classAtt
2	...	1	0	...		...		0	...	...		Memo 2	...		Auto correct setting Change settings Updatec
3	...	1	0	...		...		0	...	...		Attend seminar	...		Take notesSignificant papersGive report
4	...	1	0	...		...		0	...	...		Nemours	...		Auto correct changes spelling

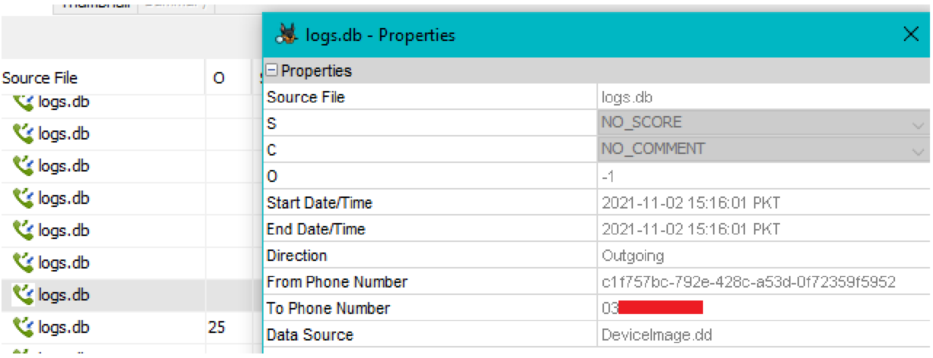
Table 5.7 – Autopsy Test Result MDT-04

Test case id	MDT-05
Test case result	As expected
Test case analysis	Autopsy was able to show the incoming call data.
Screenshots	

logs.db
logs.db
logs.db
logs.db
logs.db
logs.db
logs.db
logs.db 25

Source File	logs.db
S	NO_SCORE
C	NO_COMMENT
O	25
Start Date/Time	2021-11-02 15:14:37 PKT
End Date/Time	2021-11-02 15:14:37 PKT
Direction	Incoming
From Phone Number	03[redacted]
To Phone Number	c1f757bc-792e-428c-a53d-0f72359f5952
Data Source	DeviceImage.dd

Table 5.8– Autopsy Test Result MDT-05

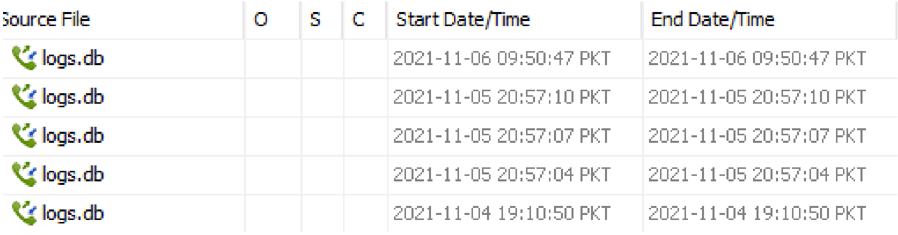
Test case id	MDT-06, MDT-08
Test case result	As expected
Test case analysis	Autopsy was able to show the outgoing call data.
Screenshots	

Source File	O
logs.db	
logs.db	
logs.db	
logs.db	
logs.db	
logs.db	
logs.db	
logs.db	25

logs.db - Properties

Properties	
Source File	logs.db
S	NO_SCORE
C	NO_COMMENT
O	-1
Start Date/Time	2021-11-02 15:16:01 PKT
End Date/Time	2021-11-02 15:16:01 PKT
Direction	Outgoing
From Phone Number	c1f757bc-792e-428c-a53d-0f72359f5952
To Phone Number	03[redacted]
Data Source	DeviceImage.dd

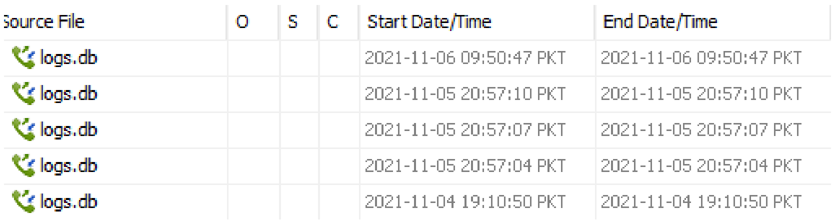
Table5.9– Autopsy Test Result MDT-06, MDT-08

Test case id	MDT-07
Test case result	As expected
Test case analysis	Autopsy was able to show the missed call data.
Screenshots	

Source File	O	S	C	Start Date/Time	End Date/Time
logs.db				2021-11-06 09:50:47 PKT	2021-11-06 09:50:47 PKT
logs.db				2021-11-05 20:57:10 PKT	2021-11-05 20:57:10 PKT
logs.db				2021-11-05 20:57:07 PKT	2021-11-05 20:57:07 PKT
logs.db				2021-11-05 20:57:04 PKT	2021-11-05 20:57:04 PKT
logs.db				2021-11-04 19:10:50 PKT	2021-11-04 19:10:50 PKT

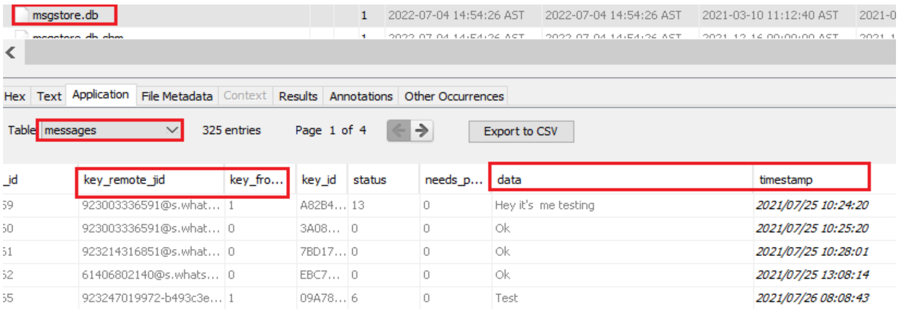
Table 5.10– Autopsy Test Result MDT-07

Test case id	MDT-09
Test case result	As expected
Test case analysis	Autopsy was able to show the duration of calls.

Screenshots	

Source File	O	S	C	Start Date/Time	End Date/Time
logs.db				2021-11-06 09:50:47 PKT	2021-11-06 09:50:47 PKT
logs.db				2021-11-05 20:57:10 PKT	2021-11-05 20:57:10 PKT
logs.db				2021-11-05 20:57:07 PKT	2021-11-05 20:57:07 PKT
logs.db				2021-11-05 20:57:04 PKT	2021-11-05 20:57:04 PKT
logs.db				2021-11-04 19:10:50 PKT	2021-11-04 19:10:50 PKT

Table 5.11– Autopsy Test Result MDT-09

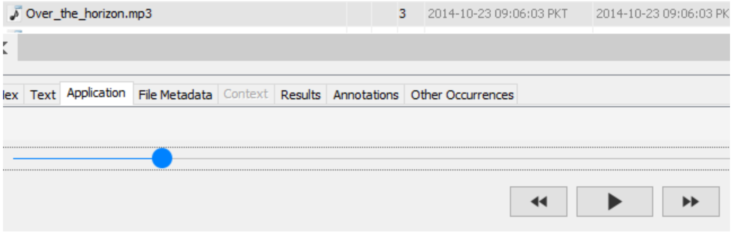
Test case id	MDT-12, MDT-15
Test case result	As expected
Test case analysis	Autopsy was able to show instant messages with time stamps.
Screenshots	

msgstore.db			1	2022-07-04 14:54:26 AST	2022-07-04 14:54:26 AST	2021-03-10 11:12:40 AST	2021-0

Table messages 325 entries Page 1 of 4

_id	key_remote_jid	key_fro...	key_id	status	needs_p...	data	timestamp
59	923003336591@s.what...	1	A82B4...	13	0	Hey it's me testing	*2021/07/25 10:24:20*
50	923003336591@s.what...	0	3A08...	0	0	Ok	*2021/07/25 10:25:20*
51	923214316851@s.what...	0	7BD17...	0	0	Ok	*2021/07/25 10:28:01*
52	61406802140@s.whats...	0	EBC7...	0	0	Ok	*2021/07/25 13:08:14*
55	923247019972-b493c3e...	1	09A78...	6	0	Test	*2021/07/26 08:08:43*

Table 5.12– Autopsy Test Result MDT-12, MDT-15

Test case id	MDT-16
Test case result	As expected
Test case analysis	Autopsy was able to show and play the audio files.
Screenshots	

Over_the_horizon.mp3			3	2014-10-23 09:06:03 PKT	2014-10-23 09:06:03 PK

Table 5.13– Autopsy Test Result MDT-16

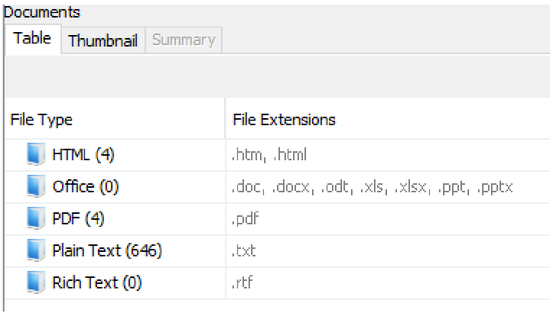
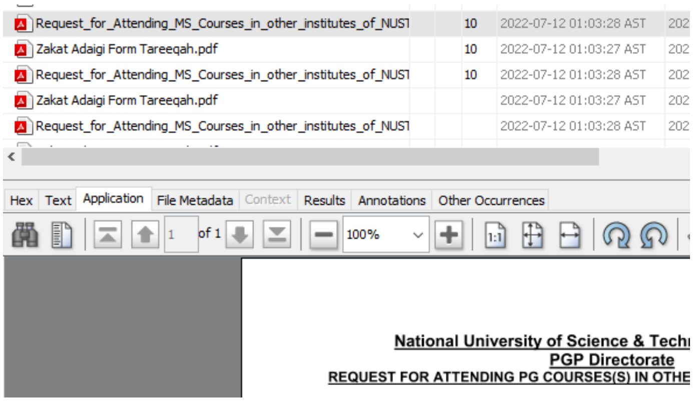
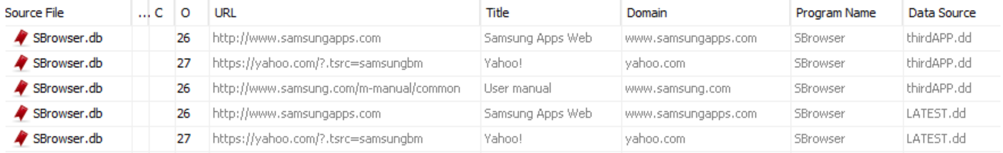
Test case id	MDT-18
Test case result	As expected
Test case analysis	Autopsy was able to show and open the documents,
Screenshots	 Documents Table · Thumbnail · Summary File Type — File Extensions HTML (4) — .htm, .html Office (0) — .doc, .docx, .odt, .xls, .xlsx, .ppt, .pptx PDF (4) — .pdf Plain Text (646) — .txt Rich Text (0) — .rtf  Request_for_Attending_MS_Courses_in_other_institutes_of_NUST — 10 — 2022-07-12 01:03:28 AST — 202 Zakat Adaigi Form Tareeqah.pdf — 10 — 2022-07-12 01:03:27 AST — 202 Request_for_Attending_MS_Courses_in_other_institutes_of_NUST — 10 — 2022-07-12 01:03:28 AST — 202 Zakat Adaigi Form Tareeqah.pdf — 2022-07-12 01:03:27 AST — 202 Request_for_Attending_MS_Courses_in_other_institutes_of_NUST — 2022-07-12 01:03:28 AST — 202 Hex · Text · Application · File Metadata · Context · Results · Annotations · Other Occurrences 1 of 1 · 100% National University of Science & Techı PGP Directorate REQUEST FOR ATTENDING PG COURSES(S) IN OTHE

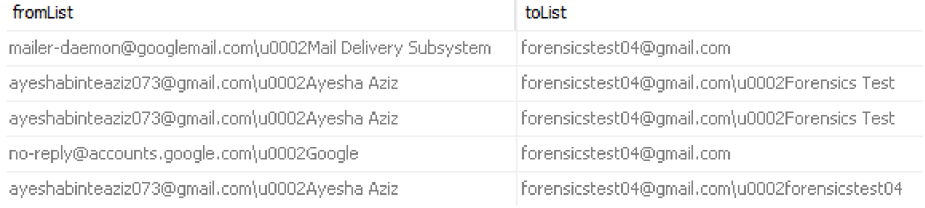
Table 5.14– Autopsy Test Result MDT-18

Test case id	MDT-21
Test case result	As expected
Test case analysis	Autopsy was able to present the bookmarks.

Screenshots	

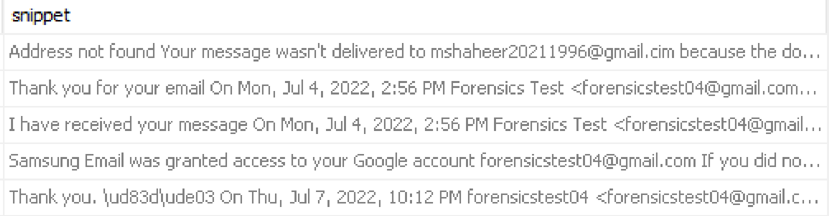
Source File	... C	O	URL	Title	Domain	Program Name	Data Source
SBrowser.db		26	http://www.samsungapps.com	Samsung Apps Web	www.samsungapps.com	SBrowser	thirdAPP.dd
SBrowser.db		27	https://yahoo.com/?.tsrc=samsungbm	Yahoo!	yahoo.com	SBrowser	thirdAPP.dd
SBrowser.db		26	http://www.samsung.com/m-manual/common	User manual	www.samsung.com	SBrowser	thirdAPP.dd
SBrowser.db		26	http://www.samsungapps.com	Samsung Apps Web	www.samsungapps.com	SBrowser	LATEST.dd
SBrowser.db		27	https://yahoo.com/?.tsrc=samsungbm	Yahoo!	yahoo.com	SBrowser	LATEST.dd

Table 5.15– Autopsy Test Result MDT-21

Test case id	MDT-22, MDT-23
Test case result	As expected
Test case analysis	Autopsy successfully presented the sender and receiver of an email.
Screenshots	

fromList	toList
mailer-daemon@googlemail.com\u0002Mail Delivery Subsystem	forensicstest04@gmail.com
ayeshabinteaziz073@gmail.com\u0002Ayesha Aziz	forensicstest04@gmail.com\u0002Forensics Test
ayeshabinteaziz073@gmail.com\u0002Ayesha Aziz	forensicstest04@gmail.com\u0002Forensics Test
no-reply@accounts.google.com\u0002Google	forensicstest04@gmail.com
ayeshabinteaziz073@gmail.com\u0002Ayesha Aziz	forensicstest04@gmail.com\u0002forensicstest04

Table 5.16– Autopsy Test Result MDT-22, MDT-23

Test case id	MDT-24
Test case result	As expected
Test case analysis	Autopsy was able to present the content of an email.
Screenshots	

snippet
Address not found Your message wasn't delivered to mshaheer20211996@gmail.cim because the do...
Thank you for your email On Mon, Jul 4, 2022, 2:56 PM Forensics Test <forensicstest04@gmail.com...
I have received your message On Mon, Jul 4, 2022, 2:56 PM Forensics Test <forensicstest04@gmail...
Samsung Email was granted access to your Google account forensicstest04@gmail.com If you did no...
Thank you. \ud83d\ude03 On Thu, Jul 7, 2022, 10:12 PM forensicstest04 <forensicstest04@gmail.c...

Table 5.17– Autopsy Test Result MDT-24

Test case id	MDT-25
Test case result	As expected

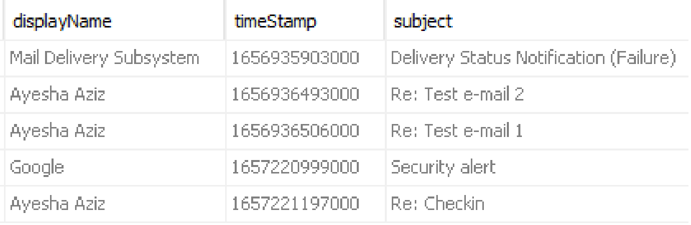
<table>
<tr><td><b>Test case analysis</b></td><td>Autopsy was able to present the timestamp of an email.</td></tr>
<tr><td><b>Screenshots</b></td><td>
<table>
<tr><th>displayName</th><th>timeStamp</th><th>subject</th></tr>
<tr><td>Mail Delivery Subsystem</td><td>1656935903000</td><td>Delivery Status Notification (Failure)</td></tr>
<tr><td>Ayesha Aziz</td><td>1656936493000</td><td>Re: Test e-mail 2</td></tr>
<tr><td>Ayesha Aziz</td><td>1656936506000</td><td>Re: Test e-mail 1</td></tr>
<tr><td>Google</td><td>1657220999000</td><td>Security alert</td></tr>
<tr><td>Ayesha Aziz</td><td>1657221197000</td><td>Re: Checkin</td></tr>
</table></td></tr>
</table>

Table 5.18– Autopsy Test Result MDT-25

WHATSAPP

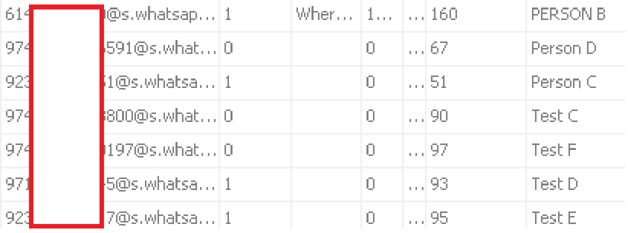
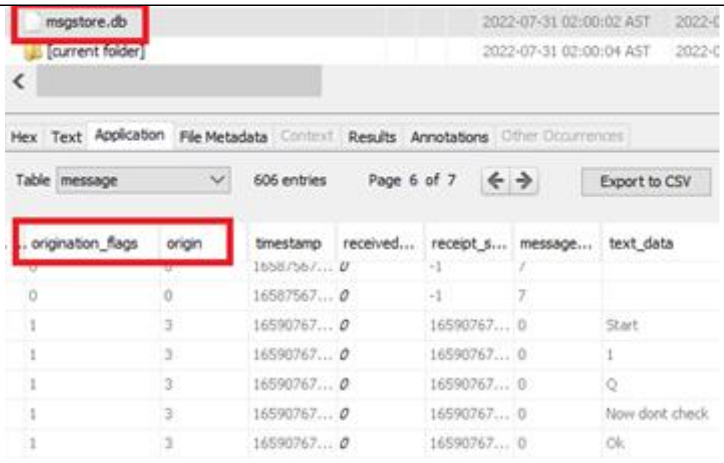
<table>
<tr><td><b>Test case id</b></td><td>MDT-26, MDT-28</td></tr>
<tr><td><b>Test case result</b></td><td>As expected</td></tr>
<tr><td><b>Test case analysis</b></td><td>Autopsy successfully presented the contact’s name and phone number within WhatsApp.</td></tr>
<tr><td><b>Screenshots</b></td><td>
<table>
<tr><td>61[redacted]@s.whatsap…</td><td>1</td><td>Wher…</td><td>1…</td><td>… 160</td><td>PERSON B</td></tr>
<tr><td>97[redacted]591@s.what…</td><td>0</td><td></td><td>0</td><td>… 67</td><td>Person D</td></tr>
<tr><td>92[redacted]1@s.whatsa…</td><td>1</td><td></td><td>0</td><td>… 51</td><td>Person C</td></tr>
<tr><td>97[redacted]800@s.what…</td><td>0</td><td></td><td>0</td><td>… 90</td><td>Test C</td></tr>
<tr><td>97[redacted]197@s.what…</td><td>0</td><td></td><td>0</td><td>… 97</td><td>Test F</td></tr>
<tr><td>97[redacted]5@s.whatsa…</td><td>1</td><td></td><td>0</td><td>… 93</td><td>Test D</td></tr>
<tr><td>92[redacted]7@s.whatsa…</td><td>1</td><td></td><td>0</td><td>… 95</td><td>Test E</td></tr>
</table></td></tr>
</table>

Table 5.19– Autopsy Test Result MDT-26, MDT-28

Test case id	MDT-37, MDT-38
Test case result	As expected
Test case analysis	Autopsy successfully presented the timestamp and chat content of a forwarded message. The origination_flags column’s value is 1 in the case of a forwarded message.

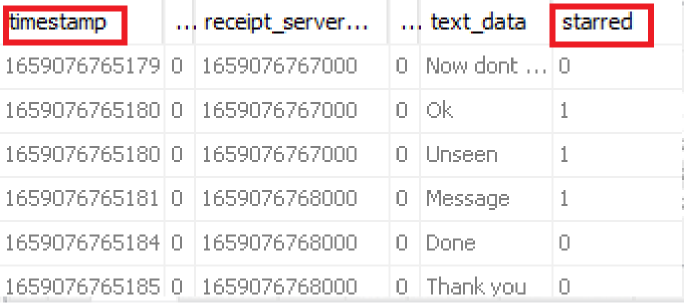
Screenshots	

msgstore.db 2022-07-31 02:00:02 AST 2022-0
[current folder] 2022-07-31 02:00:04 AST 2022-0

Table message 606 entries Page 6 of 7

… origination_flags	origin	timestamp	received…	receipt_s…	message…	text_data
0	0	16587567…	0	-1	7	
0	0	16587567…	0	-1	7	
1	3	16590767…	0	16590767…	0	Start
1	3	16590767…	0	16590767…	0	1
1	3	16590767…	0	16590767…	0	Q
1	3	16590767…	0	16590767…	0	Now dont check
1	3	16590767…	0	16590767…	0	Ok

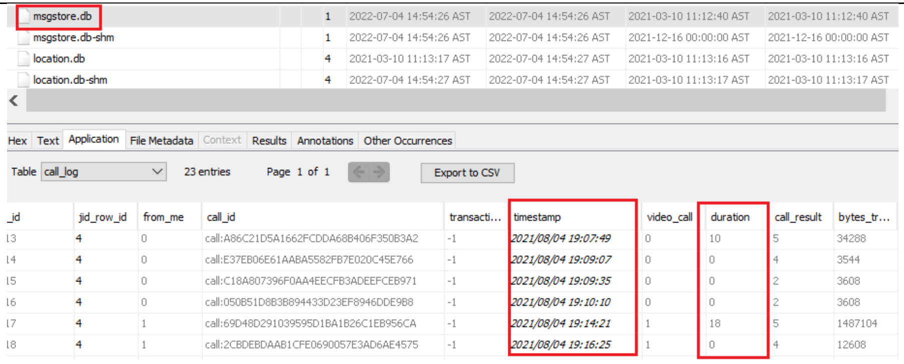
Table 5.20– Autopsy Test Result MDT-37, MDT-38

Test case id	MDT-42, MDT-43
Test case result	As expected.
Test case analysis	Autopsy successfully presented the timestamp and chat content of a starred message. The value in column “starred” is 1 in case of a starred message.
Screenshots	

timestamp	…	receipt_server…	…	text_data	starred
1659076765179	0	1659076767000	0	Now dont …	0
1659076765180	0	1659076767000	0	Ok	1
1659076765180	0	1659076767000	0	Unseen	1
1659076765181	0	1659076768000	0	Message	1
1659076765184	0	1659076768000	0	Done	0
1659076765185	0	1659076768000	0	Thank you	0

Table 5.21– Autopsy Test Result MDT-42, MDT-43

Test case id	MDT-56, MDT-57, MDT-91, MDT-92
Test case result	As expected.
Test case analysis	Autopsy successfully presented the timestamp and duration of a call.

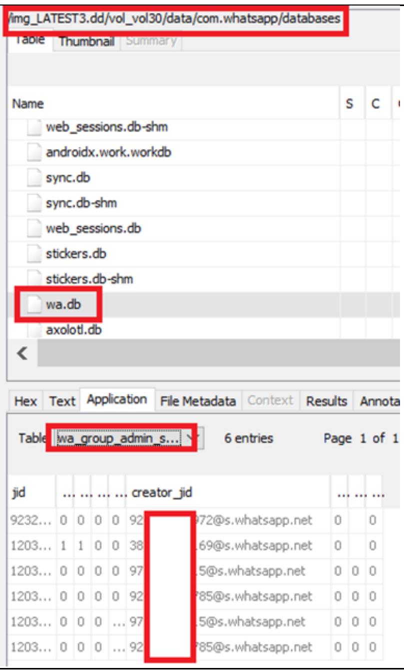
Screenshots	

msgstore.db			1	2022-07-04 14:54:26 AST	2022-07-04 14:54:26 AST	2021-03-10 11:12:40 AST	2021-03-10 11:12:40 AST
msgstore.db-shm			1	2022-07-04 14:54:26 AST	2022-07-04 14:54:26 AST	2021-12-16 00:00:00 AST	2021-12-16 00:00:00 AST
location.db			4	2021-03-10 11:13:17 AST	2022-07-04 14:54:27 AST	2021-03-10 11:13:16 AST	2021-03-10 11:13:16 AST
location.db-shm			4	2022-07-04 14:54:27 AST	2022-07-04 14:54:27 AST	2021-03-10 11:13:17 AST	2021-03-10 11:13:17 AST

Table call_log 23 entries Page 1 of 1

_id	jid_row_id	from_me	call_id	transacti…	timestamp	video_call	duration	call_result	bytes_tr…
13	4	0	call:A86C21D5A1662FCDDA68B406F350B3A2	-1	*2021/08/04 19:07:49*	0	10	5	34288
14	4	0	call:E37EB06E61AABA5582FB7E020C45E766	-1	*2021/08/04 19:09:07*	0	0	4	3544
15	4	0	call:C18A807396F0AA4EECFB3ADEEFCEB971	-1	*2021/08/04 19:09:35*	0	0	2	3608
16	4	0	call:050B51D8B3B894433D23EF8946DDE9B8	-1	*2021/08/04 19:10:10*	0	0	2	3608
17	4	1	call:69D48D291039595D1BA1B26C1EB956CA	-1	*2021/08/04 19:14:21*	1	18	5	1487104
18	4	1	call:2CBDEBDAAB1CFE0690057E3AD6AE4575	-1	*2021/08/04 19:16:25*	1	0	4	12608

Table 5.22– Autopsy Test Result MDT-56, MDT-57, MDT-91, MDT-92

Test case id	MDT-76
Test case result	As expected.
Test case analysis	Autopsy was able to extract a group admin's phone number.
Screenshots	

/img_LATEST3.dd/vol_vol30/data/com.whatsapp/databases

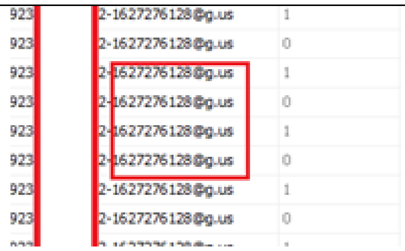
- web_sessions.db-shm
- androidx.work.workdb
- sync.db
- sync.db-shm
- web_sessions.db
- stickers.db
- stickers.db-shm
- wa.db
- axolotl.db

Table wa_group_admin_s… 6 entries Page 1 of 1

jid	…	…	…	…	creator_jid	…	…	…
9232…	0	0	0	0	92[redacted]72@s.whatsapp.net	0		0
1203…	1	1	0	0	38[redacted]69@s.whatsapp.net	0		0
1203…	0	0	0	0	97[redacted]5@s.whatsapp.net	0	0	0
1203…	0	0	0	0	92[redacted]85@s.whatsapp.net	0	0	0
1203…	0	0	0	…	97[redacted]5@s.whatsapp.net	0	0	0
1203…	0	0	0	…	92[redacted]85@s.whatsapp.net	0	0	0

Table 5.23– Autopsy Test Result MDT-76

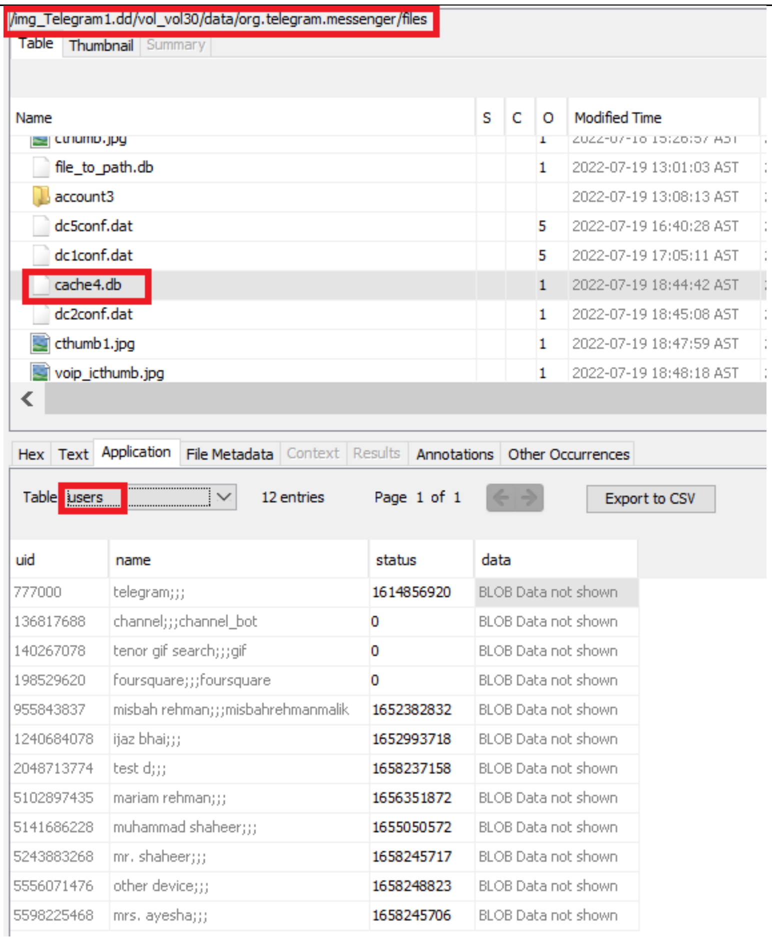
Test case id	MDT-79
Test case result	As expected.
Test case analysis	Autopsy successfully displayed the sender of a chat message

Screenshots	

923	2-1627276128@g.us	1
923	2-1627276128@g.us	0
923	2-1627276128@g.us	1
923	2-1627276128@g.us	0
923	2-1627276128@g.us	1
923	2-1627276128@g.us	0
923	2-1627276128@g.us	1
923	2-1627276128@g.us	0

Table 5.24– Autopsy Test Result MDT-79

TELEGRAM

Test case id	MDT-26
Test case result	As expected
Test case analysis	Autopsy successfully presented the contacts’ names in Telegram.
Screenshots	

/img_Telegram1.dd/vol_vol30/data/org.telegram.messenger/files

Name	S	C	O	Modified Time
cthumb.jpg			1	2022-07-18 15:26:57 AST
file_to_path.db			1	2022-07-19 13:01:03 AST
account3				2022-07-19 13:08:13 AST
dc5conf.dat			5	2022-07-19 16:40:28 AST
dc1conf.dat			5	2022-07-19 17:05:11 AST
cache4.db			1	2022-07-19 18:44:42 AST
dc2conf.dat			1	2022-07-19 18:45:08 AST
cthumb1.jpg			1	2022-07-19 18:47:59 AST
voip_icthumb.jpg			1	2022-07-19 18:48:18 AST

Table users 12 entries Page 1 of 1

uid	name	status	data
777000	telegram;;;	1614856920	BLOB Data not shown
136817688	channel;;;channel_bot	0	BLOB Data not shown
140267078	tenor gif search;;;gif	0	BLOB Data not shown
198529620	foursquare;;;foursquare	0	BLOB Data not shown
955843837	misbah rehman;;;misbahrehmanmalik	1652382832	BLOB Data not shown
1240684078	ijaz bhai;;;	1652993718	BLOB Data not shown
2048713774	test d;;;	1658237158	BLOB Data not shown
5102897435	mariam rehman;;;	1656351872	BLOB Data not shown
5141686228	muhammad shaheer;;;	1655050572	BLOB Data not shown
5243883268	mr. shaheer;;;	1658245717	BLOB Data not shown
5556071476	other device;;;	1658248823	BLOB Data not shown
5598225468	mrs. ayesha;;;	1658245706	BLOB Data not shown

Table 5.25– Autopsy Test Result MDT-26

Test case id	MDT-27

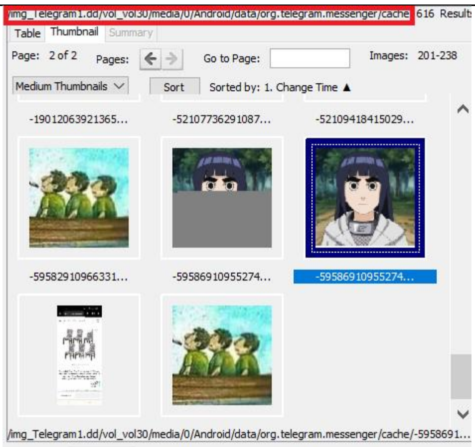
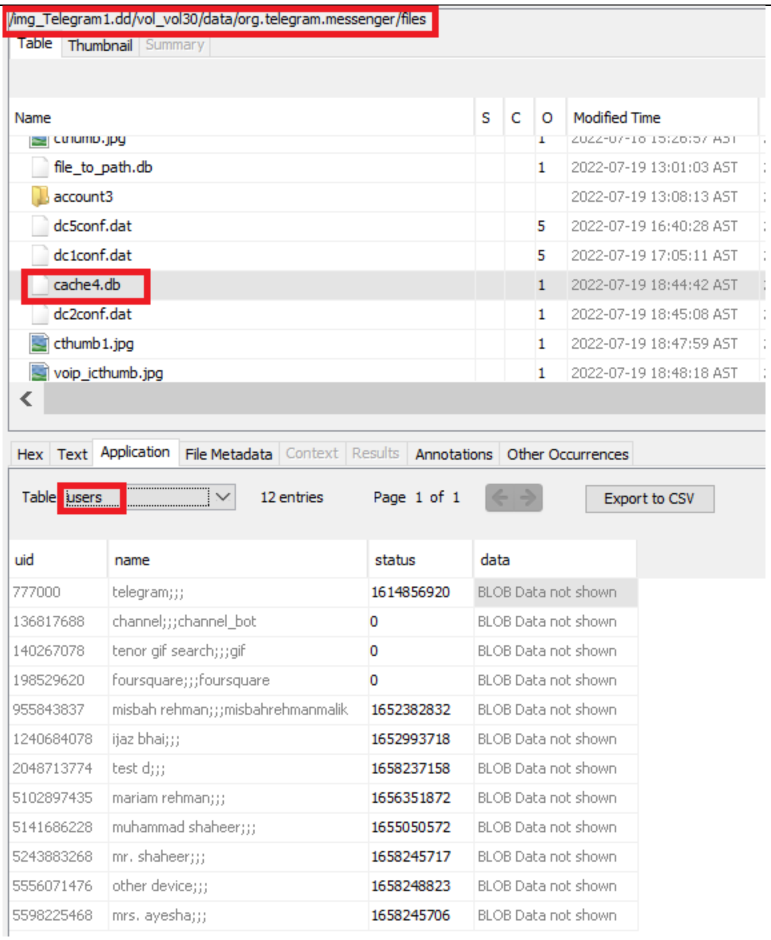
Test case result	As expected
Test case analysis	Autopsy was able to present the cached profile picture of the telegram’s contacts.
Screenshots	 /img_Telegram1.dd/vol_vol30/media/0/Android/data/org.telegram.messenger/cache 616 Result Table Thumbnail Summary Page: 2 of 2 Pages: Go to Page: Images: 201-238 Medium Thumbnails Sort Sorted by: 1. Change Time ▲ -19012063921365... -52107736291087... -52109418415029... -59582910966331... -59586910955274... -59586910955274... /img_Telegram1.dd/vol_vol30/media/0/Android/data/org.telegram.messenger/cache/-5958691...

Table 5.26– Autopsy Test Result MDT-27

Test case id	MDT-28
Test case result	As expected.
Test case analysis	Autopsy was unable to decode the contact numbers as they were stored in BLOB format.

Screenshots	

/img_Telegram1.dd/vol_vol30/data/org.telegram.messenger/files

Name	S	C	O	Modified Time
cthumb.jpg			1	2022-07-18 15:26:57 AST
file_to_path.db			1	2022-07-19 13:01:03 AST
account3				2022-07-19 13:08:13 AST
dc5conf.dat			5	2022-07-19 16:40:28 AST
dc1conf.dat			5	2022-07-19 17:05:11 AST
cache4.db			1	2022-07-19 18:44:42 AST
dc2conf.dat			1	2022-07-19 18:45:08 AST
cthumb1.jpg			1	2022-07-19 18:47:59 AST
voip_icthumb.jpg			1	2022-07-19 18:48:18 AST

Table users

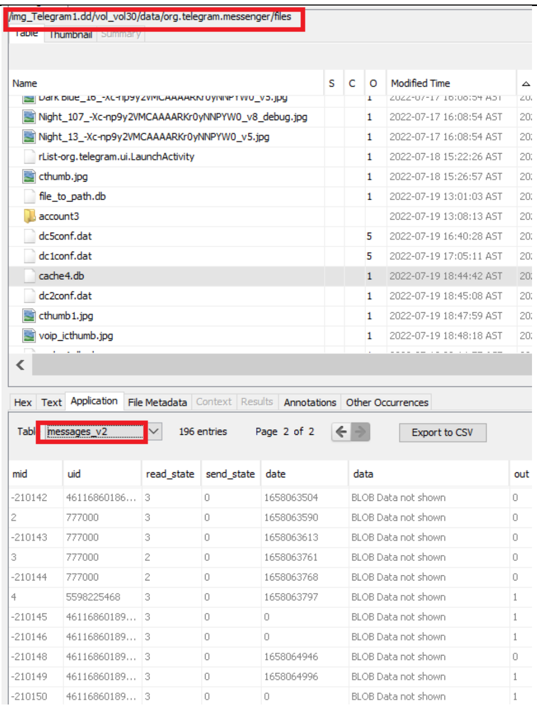
12 entries

Page 1 of 1

uid	name	status	data
777000	telegram;;;	1614856920	BLOB Data not shown
136817688	channel;;;channel_bot	0	BLOB Data not shown
140267078	tenor gif search;;;gif	0	BLOB Data not shown
198529620	foursquare;;;foursquare	0	BLOB Data not shown
955843837	misbah rehman;;;misbahrehmanmalik	1652382832	BLOB Data not shown
1240684078	ijaz bhai;;;	1652993718	BLOB Data not shown
2048713774	test d;;;	1658237158	BLOB Data not shown
5102897435	mariam rehman;;;	1656351872	BLOB Data not shown
5141686228	muhammad shaheer;;;	1655050572	BLOB Data not shown
5243883268	mr. shaheer;;;	1658245717	BLOB Data not shown
5556071476	other device;;;	1658248823	BLOB Data not shown
5598225468	mrs. ayesha;;;	1658245706	BLOB Data not shown

Table 5.27– Autopsy Test Result MDT-28

Test case id	MDT-33, MDT-104, MDT-113
Test case result	As expected
Test case analysis	Autopsy successfully displayed the timestamp of the chat messages of the Telegram app.

Screenshots	

/img_Telegram1.dd/vol_vol30/data/org.telegram.messenger/files

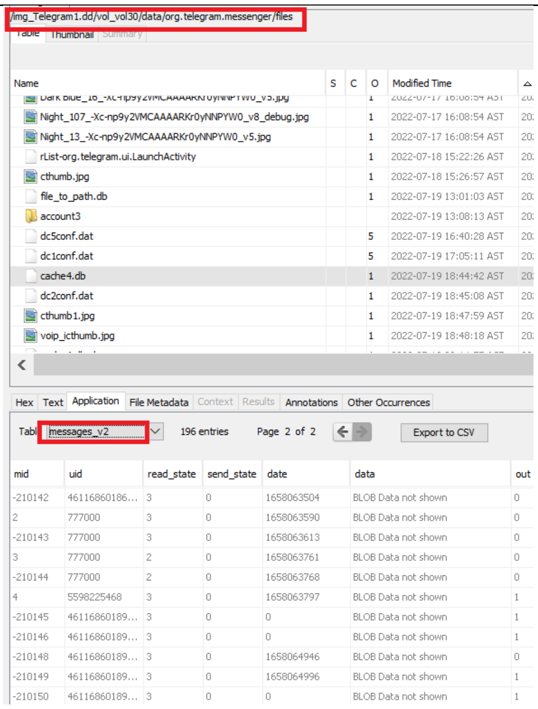
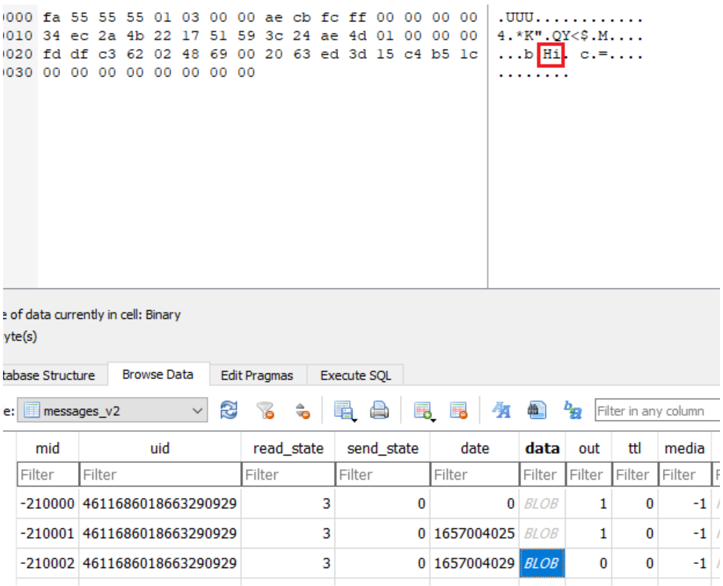
Name	S	C	O	Modified Time
Dark Blue_16_-Xc-np9y2VMCAAAARKr0yNNPYW0_v5.jpg			1	2022-07-17 16:08:54 AST
Night_107_-Xc-np9y2VMCAAAARKr0yNNPYW0_v8_debug.jpg			1	2022-07-17 16:08:54 AST
Night_13_-Xc-np9y2VMCAAAARKr0yNNPYW0_v5.jpg			1	2022-07-17 16:08:54 AST
rList-org.telegram.ui.LaunchActivity			1	2022-07-18 15:22:26 AST
cthumb.jpg			1	2022-07-18 15:26:57 AST
file_to_path.db			1	2022-07-19 13:01:03 AST
account3				2022-07-19 13:08:13 AST
dc5conf.dat			5	2022-07-19 16:40:28 AST
dc1conf.dat			5	2022-07-19 17:05:11 AST
cache4.db			1	2022-07-19 18:44:42 AST
dc2conf.dat			1	2022-07-19 18:45:08 AST
cthumb1.jpg			1	2022-07-19 18:47:59 AST
voip_icthumb.jpg			1	2022-07-19 18:48:18 AST

Tabl messages_v2 196 entries Page 2 of 2

mid	uid	read_state	send_state	date	data	out
-210142	46116860186…	3	0	1658063504	BLOB Data not shown	0
2	777000	3	0	1658063590	BLOB Data not shown	0
-210143	777000	3	0	1658063613	BLOB Data not shown	0
3	777000	2	0	1658063761	BLOB Data not shown	0
-210144	777000	2	0	1658063768	BLOB Data not shown	0
4	5598225468	3	0	1658063797	BLOB Data not shown	1
-210145	46116860189…	3	0	0	BLOB Data not shown	1
-210146	46116860189…	3	0	0	BLOB Data not shown	1
-210148	46116860189…	3	0	1658064946	BLOB Data not shown	0
-210149	46116860189…	3	0	1658064996	BLOB Data not shown	1
-210150	46116860189…	3	0	0	BLOB Data not shown	1

Table 5.28– Autopsy Test Result MDT-33, MDT-104, MDT-113

Test case id	MDT-34, MDT-38, MDT-105, MDT-114
Test case result	Successful in combination with the SQLite browser.
Test case analysis	Autopsy was unable to display the chat content of a message stored in BLOB format. Although, after extracting cache4.db database from Autopsy, it can be viewed via SQLite DB Browser.

Screenshots	 

/img_Telegram1.dd/vol_vol30/data/org.telegram.messenger/files

Name	S	C	O	Modified Time
Dark Blue_16_-Xc-np9y2VMCAAAARKr0yNNPYW0_v5.jpg			1	2022-07-17 16:08:54 AST
Night_107_-Xc-np9y2VMCAAAARKr0yNNPYW0_v8_debug.jpg			1	2022-07-17 16:08:54 AST
Night_13_-Xc-np9y2VMCAAAARKr0yNNPYW0_v5.jpg			1	2022-07-17 16:08:54 AST
rList-org.telegram.ui.LaunchActivity			1	2022-07-18 15:22:26 AST
cthumb.jpg			1	2022-07-18 15:26:57 AST
file_to_path.db			1	2022-07-19 13:01:03 AST
account3				2022-07-19 13:08:13 AST
dc5conf.dat			5	2022-07-19 16:40:28 AST
dc1conf.dat			5	2022-07-19 17:05:11 AST
cache4.db			1	2022-07-19 18:44:42 AST
dc2conf.dat			1	2022-07-19 18:45:08 AST
cthumb1.jpg			1	2022-07-19 18:47:59 AST
voip_icthumb.jpg			1	2022-07-19 18:48:18 AST

Tabl messages_v2 196 entries Page 2 of 2

mid	uid	read_state	send_state	date	data	out
-210142	46116860186...	3	0	1658063504	BLOB Data not shown	0
2	777000	3	0	1658063590	BLOB Data not shown	0
-210143	777000	3	0	1658063613	BLOB Data not shown	0
3	777000	2	0	1658063761	BLOB Data not shown	0
-210144	777000	2	0	1658063768	BLOB Data not shown	0
4	5598225468	3	0	1658063797	BLOB Data not shown	1
-210145	46116860189...	3	0	0	BLOB Data not shown	1
-210146	46116860189...	3	0	0	BLOB Data not shown	1
-210148	46116860189...	3	0	1658064946	BLOB Data not shown	0
-210149	46116860189...	3	0	1658064996	BLOB Data not shown	1
-210150	46116860189...	3	0	0	BLOB Data not shown	1

```
000 fa 55 55 55 01 03 00 00 ae cb fc ff 00 00 00 00   .UUU............
010 34 ec 2a 4b 22 17 51 59 3c 24 ae 4d 01 00 00 00   4.*K".QY<$.M....
020 fd df c3 62 02 48 69 00 20 63 ed 3d 15 c4 b5 1c   ...b.Hi. c.=....
030 00 00 00 00 00 00 00 00                           ........
```

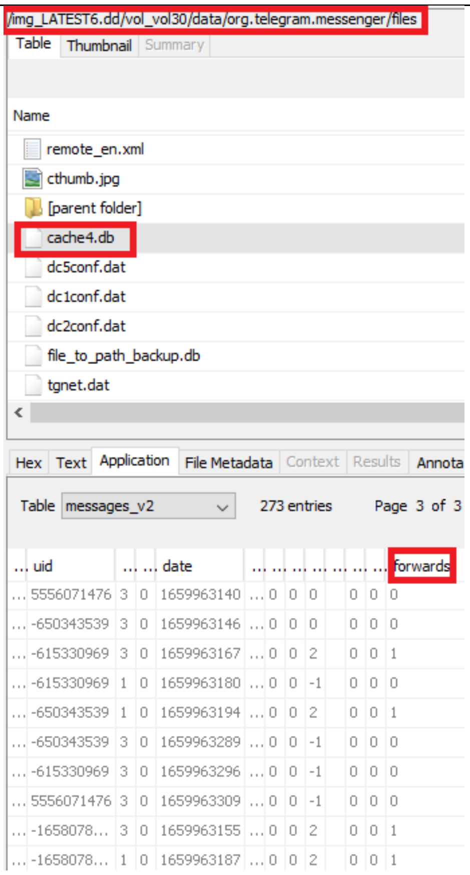
e of data currently in cell: Binary
yte(s)

e: messages_v2

mid	uid	read_state	send_state	date	data	out	ttl	media
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
-210000	4611686018663290929	3	0	0	BLOB	1	0	-1
-210001	4611686018663290929	3	0	1657004025	BLOB	1	0	-1
-210002	4611686018663290929	3	0	1657004029	BLOB	0	0	-1

Table 5.29– Autopsy Test Result MDT-34, MDT-38, MDT-105, MDT-114

Test case id	MDT-37
Test case result	As expected
Test case analysis	Autopsy successfully displayed the timestamp of the forwarded chat messages of the Telegram app.

Screenshots	

/img_LATEST6.dd/vol_vol30/data/org.telegram.messenger/files

Table Thumbnail Summary

Name

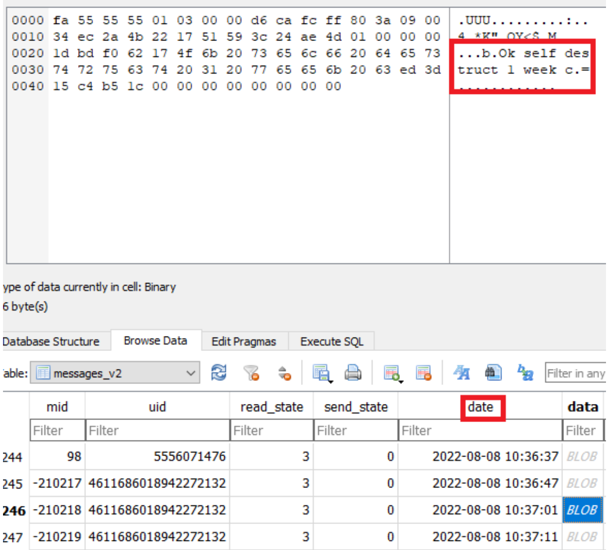
- remote_en.xml
- cthumb.jpg
- [parent folder]
- cache4.db
- dc5conf.dat
- dc1conf.dat
- dc2conf.dat
- file_to_path_backup.db
- tgnet.dat

Hex Text Application File Metadata Context Results Annota

Table messages_v2 273 entries Page 3 of 3

…	uid	…	…	date	…	…	…	…	…	…	…	forwards
…	5556071476	3	0	1659963140	…	0	0	0		0	0	0
…	-650343539	3	0	1659963146	…	0	0	0		0	0	0
…	-615330969	3	0	1659963167	…	0	0	2		0	0	1
…	-615330969	1	0	1659963180	…	0	0	-1		0	0	0
…	-650343539	1	0	1659963194	…	0	0	2		0	0	1
…	-650343539	3	0	1659963289	…	0	0	-1		0	0	0
…	-615330969	3	0	1659963296	…	0	0	-1		0	0	0
…	5556071476	3	0	1659963309	…	0	0	-1		0	0	0
…	-1658078…	3	0	1659963155	…	0	0	2		0	0	1
…	-1658078…	1	0	1659963187	…	0	0	2		0	0	1

Table 5.30– Autopsy Test Result MDT-37

Test case id	MDT-46, MDT-47, MDT-82, MDT-83
Test case result	As expected.
Test case analysis	Autopsy successfully displayed the timestamp and chat content of a disappearing message.
Screenshots	

```
0000 fa 55 55 55 01 03 00 00 d6 ca fc ff 80 3a 09 00   .UUU.........:..
0010 34 ec 2a 4b 22 17 51 59 3c 24 ae 4d 01 00 00 00   4 *K" QY<$ M
0020 1d bd f0 62 17 4f 6b 20 73 65 6c 66 20 64 65 73   ...b.Ok self des
0030 74 72 75 63 74 20 31 20 77 65 65 6b 20 63 ed 3d   truct 1 week c.=
0040 15 c4 b5 1c 00 00 00 00 00 00 00 00               ............
```

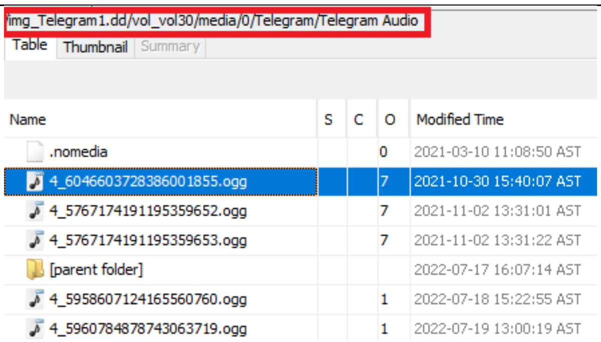
ype of data currently in cell: Binary
6 byte(s)

Database Structure Browse Data Edit Pragmas Execute SQL

able: messages_v2 Filter in any

	mid	uid	read_state	send_state	date	data
	Filter	Filter	Filter	Filter	Filter	Filter
244	98	5556071476	3	0	2022-08-08 10:36:37	BLOB
245	-210217	4611686018942272132	3	0	2022-08-08 10:36:47	BLOB
246	-210218	4611686018942272132	3	0	2022-08-08 10:37:01	BLOB
247	-210219	4611686018942272132	3	0	2022-08-08 10:37:11	BLOB

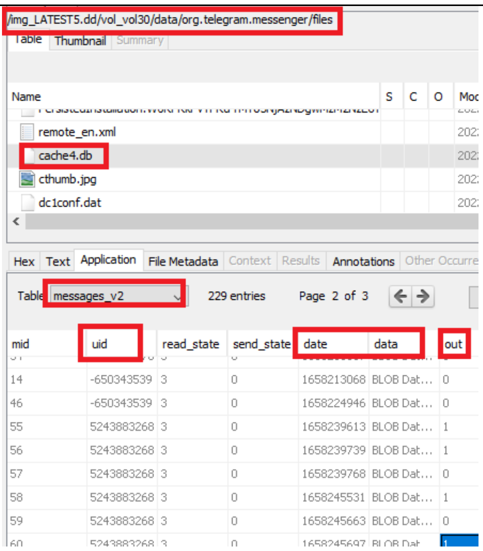
Table 5.31– Autopsy Test Result MDT-46, MDT-47, MDT-82, MDT-83

Test case id	MDT-52, MDT-53, MDT-87, MDT-88, MDT-106, MDT-107
Test case result	As expected.
Test case analysis	Autopsy successfully displayed the timestamp and content of a voice message.
Screenshots	

/img_Telegram1.dd/vol_vol30/media/0/Telegram/Telegram Audio

Name	S	C	O	Modified Time
.nomedia			0	2021-03-10 11:08:50 AST
4_6046603728386001855.ogg			7	2021-10-30 15:40:07 AST
4_5767174191195359652.ogg			7	2021-11-02 13:31:01 AST
4_5767174191195359653.ogg			7	2021-11-02 13:31:22 AST
[parent folder]				2022-07-17 16:07:14 AST
4_5958607124165560760.ogg			1	2022-07-18 15:22:55 AST
4_5960784878743063719.ogg			1	2022-07-19 13:00:19 AST

Table 5.32– Autopsy Test Result MDT-52, MDT-53, MDT-87, MDT-88, MDT-106, MDT-107

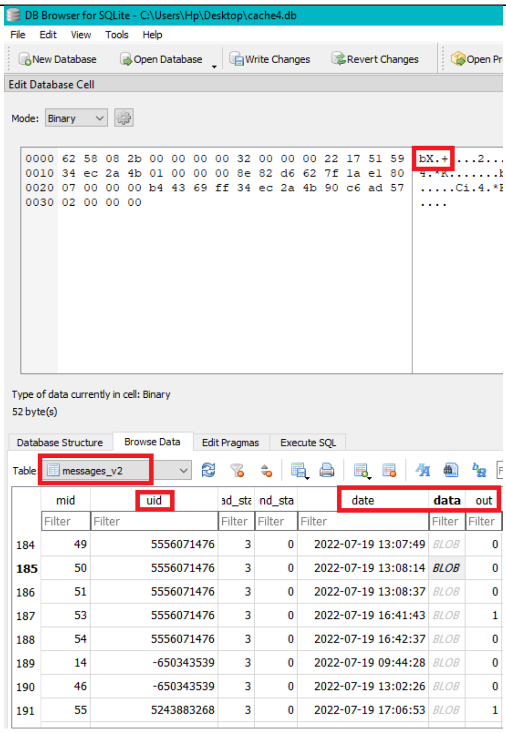
Test case id	MDT-56, MDT-60, MDT-91, MDT-95
Test case result	Successful in combination with the SQLite browser.
Test case analysis	Autopsy successfully displayed the timestamp of a voice call and a video call but it detected a call with the help of the SQLite browser.
Screenshots	

/img_LATEST5.dd/vol_vol30/data/org.telegram.messenger/files

Name	S	C	O	Moc
remote_en.xml				202
cache4.db				202
cthumb.jpg				202
dc1conf.dat				202

Table messages_v2 229 entries Page 2 of 3

mid	uid	read_state	send_state	date	data	out
14	-650343539	3	0	1658213068	BLOB Dat...	0
46	-650343539	3	0	1658224946	BLOB Dat...	0
55	5243883268	3	0	1658239613	BLOB Dat...	1
56	5243883268	3	0	1658239739	BLOB Dat...	1
57	5243883268	3	0	1658239768	BLOB Dat...	0
58	5243883268	3	0	1658245531	BLOB Dat...	1
59	5243883268	3	0	1658245663	BLOB Dat...	0
60	5243883268	3	0	1658245697	BLOB Dat	1

DB Browser for SQLite - C:\Users\Hp\Desktop\cache4.db

Edit Database Cell

Mode: Binary

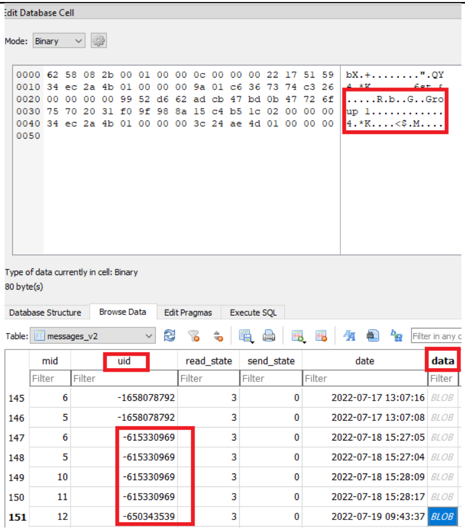
```
0000 62 58 08 2b 00 00 00 00 32 00 00 00 22 17 51 59  bX.+ ...2...
0010 34 ec 2a 4b 01 00 00 00 8e 82 d6 62 7f 1a e1 80  4.*K.......k
0020 07 00 00 00 b4 43 69 ff 34 ec 2a 4b 90 c6 ad 57  .....Ci.4.*E
0030 02 00 00 00                                      ....
```

Type of data currently in cell: Binary
52 byte(s)

Table: messages_v2

	mid	uid	ad_sta	nd_sta	date	data	out
	Filter	Filter	Filter	Filter	Filter	Filter	Filter
184	49	5556071476	3	0	2022-07-19 13:07:49	BLOB	0
185	50	5556071476	3	0	2022-07-19 13:08:14	BLOB	0
186	51	5556071476	3	0	2022-07-19 13:08:37	BLOB	0
187	53	5556071476	3	0	2022-07-19 16:41:43	BLOB	1
188	54	5556071476	3	0	2022-07-19 16:42:37	BLOB	0
189	14	-650343539	3	0	2022-07-19 09:44:28	BLOB	0
190	46	-650343539	3	0	2022-07-19 13:02:26	BLOB	0
191	55	5243883268	3	0	2022-07-19 17:06:53	BLOB	1

Table 5.33– Autopsy Test Result MDT-56, MDT-60, MDT-91, MDT-95

Test case id	MDT-75
Test case result	Successful in combination with the SQLite browser.
Test case analysis	Autopsy successfully displayed the time when a group was created.
Screenshots	

Edit Database Cell

Mode: Binary

```
0000 62 58 08 2b 00 01 00 00 0c 00 00 00 22 17 51 59  bX.+........".QY
0010 34 ec 2a 4b 01 00 00 00 9a 01 c6 36 73 74 c3 26  4.*K......6st.&
0020 00 00 00 00 99 52 d6 62 ad cb 47 bd 0b 47 72 6f  .....R.b..G..Gro
0030 75 70 20 31 f0 9f 98 8a 15 c4 b5 1c 02 00 00 00  up 1...........
0040 34 ec 2a 4b 01 00 00 00 3c 24 ae 4d 01 00 00 00  4.*K....<$.M....
0050
```

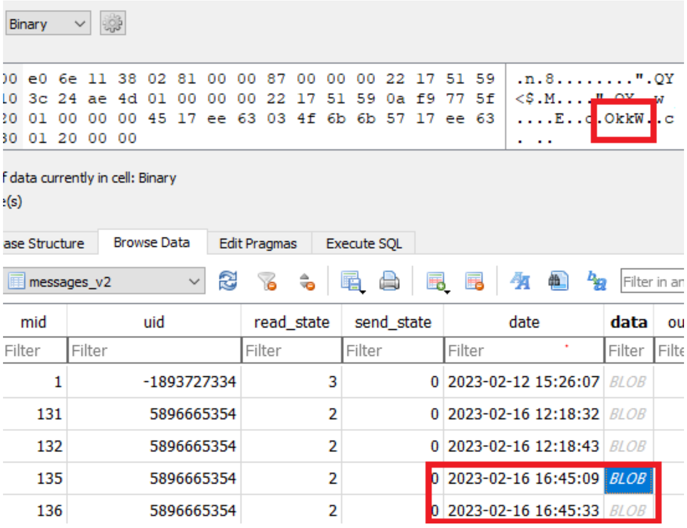
Type of data currently in cell: Binary
80 byte(s)

Table: messages_v2

	mid	uid	read_state	send_state	date	data
	Filter	Filter	Filter	Filter	Filter	Filter
145	6	-1658078792	3	0	2022-07-17 13:07:16	BLOB
146	5	-1658078792	3	0	2022-07-17 13:07:08	BLOB
147	6	-615330969	3	0	2022-07-18 15:27:05	BLOB
148	5	-615330969	3	0	2022-07-18 15:27:04	BLOB
149	10	-615330969	3	0	2022-07-18 15:28:09	BLOB
150	11	-615330969	3	0	2022-07-18 15:28:17	BLOB
151	12	-650343539	3	0	2022-07-19 09:43:37	BLOB

Table 5.34– Autopsy Test Result MDT-75

Test case id	MDT-117, MDT-118

Test case result	Successful in combination with the SQLite browser.
Test case analysis	The timestamp and chat content of an edited message were successfully recovered by autopsy.
Screenshots	

```
)0 e0 6e 11 38 02 81 00 00 87 00 00 00 22 17 51 59   .n.8........".QY
L0 3c 24 ae 4d 01 00 00 00 22 17 51 59 0a f9 77 5f   <$.M....".QY..w
20 01 00 00 00 45 17 ee 63 03 4f 6b 6b 57 17 ee 63   ....E..c.OkkW..c
30 01 20 00 00                                       . ..
```

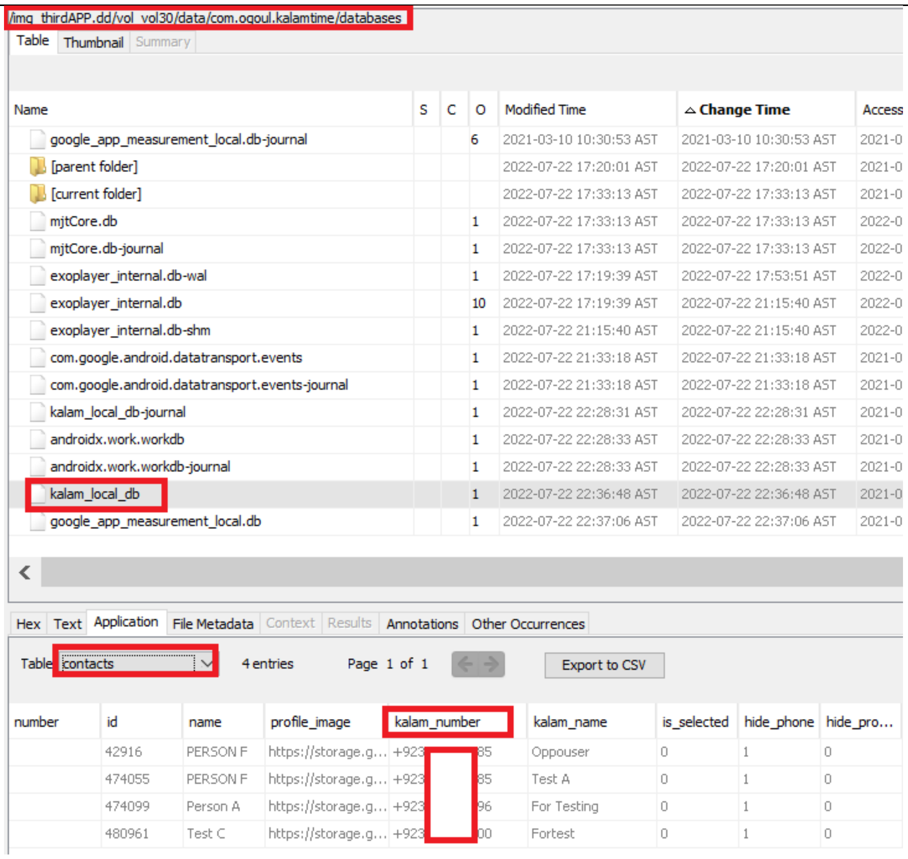
f data currently in cell: Binary
:(s)

mid	uid	read_state	send_state	date	data	ou
Filter	Filter	Filter	Filter	Filter	Filter	Filte
1	-1893727334	3	0	2023-02-12 15:26:07	BLOB	
131	5896665354	2	0	2023-02-16 12:18:32	BLOB	
132	5896665354	2	0	2023-02-16 12:18:43	BLOB	
135	5896665354	2	0	2023-02-16 16:45:09	BLOB	
136	5896665354	2	0	2023-02-16 16:45:33	BLOB	

Table 5.35– Autopsy Test Result MDT-117, MDT-118

KALAMTIME

Test case id	MDT-26, MDT-27, MDT-28
Test case result	As expected
Test case analysis	Autopsy successfully presented the contact name, profile image, and phone number from KalamTime.

Screenshots	

/img_thirdAPP.dd/vol_vol30/data/com.ogoul.kalamtime/databases

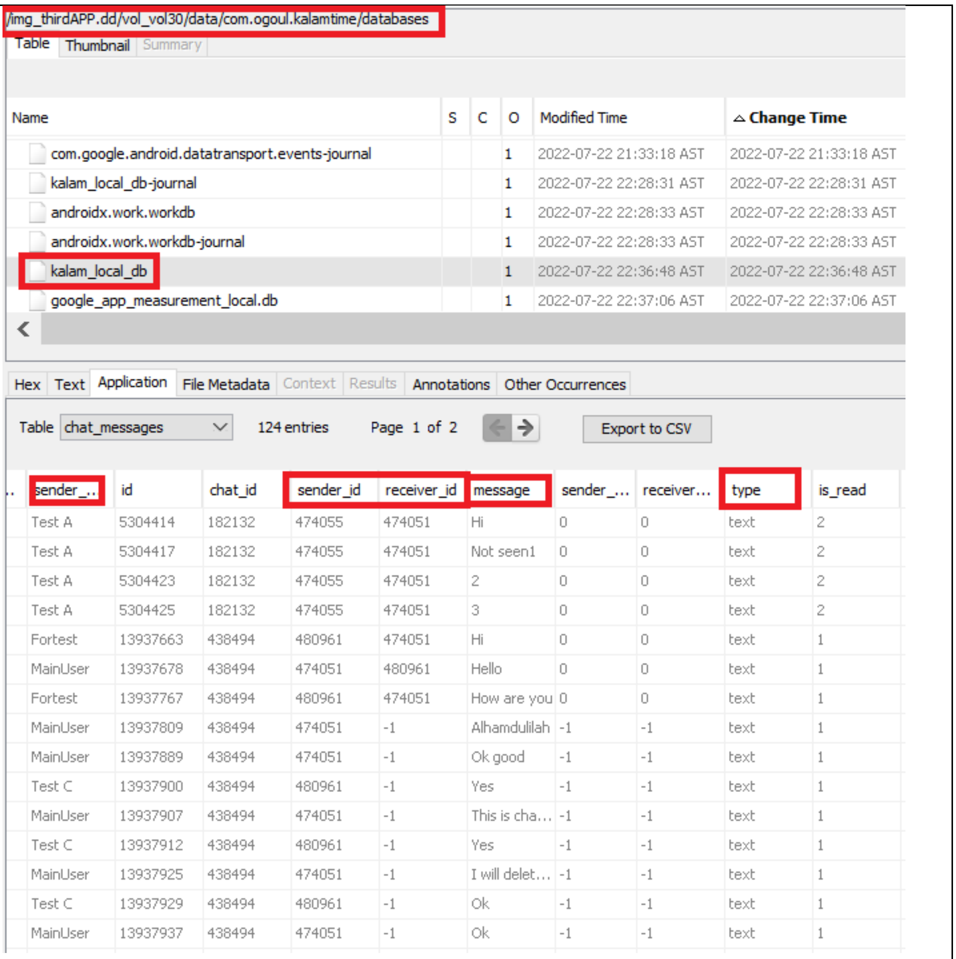
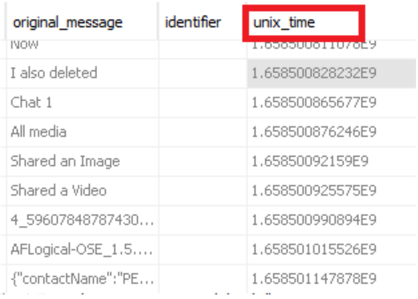
Name	S	C	O	Modified Time	Change Time	Access
google_app_measurement_local.db-journal			6	2021-03-10 10:30:53 AST	2021-03-10 10:30:53 AST	2021-0
[parent folder]				2022-07-22 17:20:01 AST	2022-07-22 17:20:01 AST	2021-0
[current folder]				2022-07-22 17:33:13 AST	2022-07-22 17:33:13 AST	2021-0
mjtCore.db			1	2022-07-22 17:33:13 AST	2022-07-22 17:33:13 AST	2022-0
mjtCore.db-journal			1	2022-07-22 17:33:13 AST	2022-07-22 17:33:13 AST	2022-0
exoplayer_internal.db-wal			1	2022-07-22 17:19:39 AST	2022-07-22 17:53:51 AST	2022-0
exoplayer_internal.db			10	2022-07-22 17:19:39 AST	2022-07-22 21:15:40 AST	2022-0
exoplayer_internal.db-shm			1	2022-07-22 21:15:40 AST	2022-07-22 21:15:40 AST	2022-0
com.google.android.datatransport.events			1	2022-07-22 21:33:18 AST	2022-07-22 21:33:18 AST	2021-0
com.google.android.datatransport.events-journal			1	2022-07-22 21:33:18 AST	2022-07-22 21:33:18 AST	2021-0
kalam_local_db-journal			1	2022-07-22 22:28:31 AST	2022-07-22 22:28:31 AST	2021-0
androidx.work.workdb			1	2022-07-22 22:28:33 AST	2022-07-22 22:28:33 AST	2021-0
androidx.work.workdb-journal			1	2022-07-22 22:28:33 AST	2022-07-22 22:28:33 AST	2021-0
kalam_local_db			1	2022-07-22 22:36:48 AST	2022-07-22 22:36:48 AST	2021-0
google_app_measurement_local.db			1	2022-07-22 22:37:06 AST	2022-07-22 22:37:06 AST	2021-0

Table contacts 4 entries Page 1 of 1

number	id	name	profile_image	kalam_number	kalam_name	is_selected	hide_phone	hide_pro...
	42916	PERSON F	https://storage.g...	+923[redacted]85	Oppouser	0	1	0
	474055	PERSON F	https://storage.g...	+923[redacted]85	Test A	0	1	0
	474099	Person A	https://storage.g...	+923[redacted]96	For Testing	0	1	0
	480961	Test C	https://storage.g...	+923[redacted]00	Fortest	0	1	0

Table 5.36– Autopsy Test Result MDT-26, MDT-27, MDT-28

Test case id	MDT-31, MDT-32, MDT-33, MDT-34
Test case result	As expected
Test case analysis	Autopsy successfully displayed the chat message’s sender, receiver, timestamp, and content in the KalamTime app.
Screenshots	

/img_thirdAPP.dd/vol_vol30/data/com.ogoul.kalamtime/databases

Table | Thumbnail | Summary

Name	S	C	O	Modified Time	Change Time
com.google.android.datatransport.events-journal			1	2022-07-22 21:33:18 AST	2022-07-22 21:33:18 AST
kalam_local_db-journal			1	2022-07-22 22:28:31 AST	2022-07-22 22:28:31 AST
androidx.work.workdb			1	2022-07-22 22:28:33 AST	2022-07-22 22:28:33 AST
androidx.work.workdb-journal			1	2022-07-22 22:28:33 AST	2022-07-22 22:28:33 AST
kalam_local_db			1	2022-07-22 22:36:48 AST	2022-07-22 22:36:48 AST
google_app_measurement_local.db			1	2022-07-22 22:37:06 AST	2022-07-22 22:37:06 AST

Hex | Text | Application | File Metadata | Context | Results | Annotations | Other Occurrences

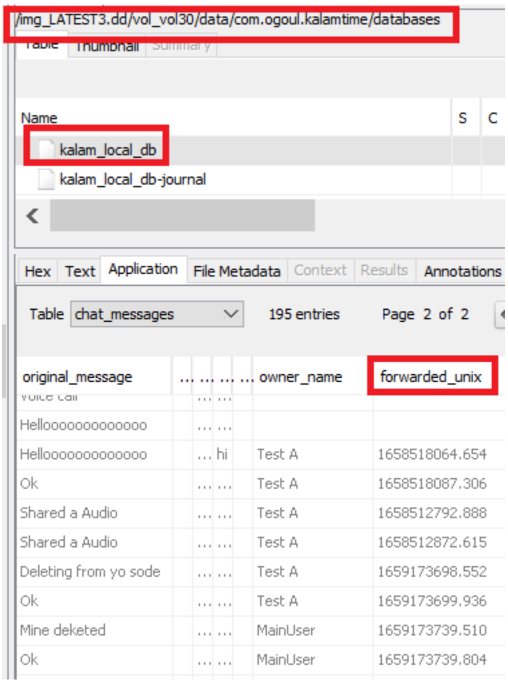
Table chat_messages | 124 entries | Page 1 of 2 | Export to CSV

sender_...	id	chat_id	sender_id	receiver_id	message	sender_...	receiver...	type	is_read
Test A	5304414	182132	474055	474051	Hi	0	0	text	2
Test A	5304417	182132	474055	474051	Not seen1	0	0	text	2
Test A	5304423	182132	474055	474051	2	0	0	text	2
Test A	5304425	182132	474055	474051	3	0	0	text	2
Fortest	13937663	438494	480961	474051	Hi	0	0	text	1
MainUser	13937678	438494	474051	480961	Hello	0	0	text	1
Fortest	13937767	438494	480961	474051	How are you	0	0	text	1
MainUser	13937809	438494	474051	-1	Alhamdulilah	-1	-1	text	1
MainUser	13937889	438494	474051	-1	Ok good	-1	-1	text	1
Test C	13937900	438494	480961	-1	Yes	-1	-1	text	1
MainUser	13937907	438494	474051	-1	This is cha...	-1	-1	text	1
Test C	13937912	438494	480961	-1	Yes	-1	-1	text	1
MainUser	13937925	438494	474051	-1	I will delet...	-1	-1	text	1
Test C	13937929	438494	480961	-1	Ok	-1	-1	text	1
MainUser	13937937	438494	474051	-1	Ok	-1	-1	text	1

original_message	identifier	unix_time
Now		1.658500811078E9
I also deleted		1.658500828232E9
Chat 1		1.658500865677E9
All media		1.658500876246E9
Shared an Image		1.65850092159E9
Shared a Video		1.658500925575E9
4_59607848787430...		1.658500990894E9
AFLogical-OSE_1.5....		1.658501015526E9
{"contactName":"PE...		1.658501147878E9

Table 5.37– Autopsy Test Result MDT-31, MDT-32, MDT-33, MDT-34

Test case id	MDT-35, MDT-36, MDT-37, MDT-38
Test case result	As expected
Test case analysis	Autopsy successfully displayed the chat message's sender, receiver, timestamp, and content in the KalamTime app.

Screenshots	

/img_LATEST3.dd/vol_vol30/data/com.ogoul.kalamtime/databases

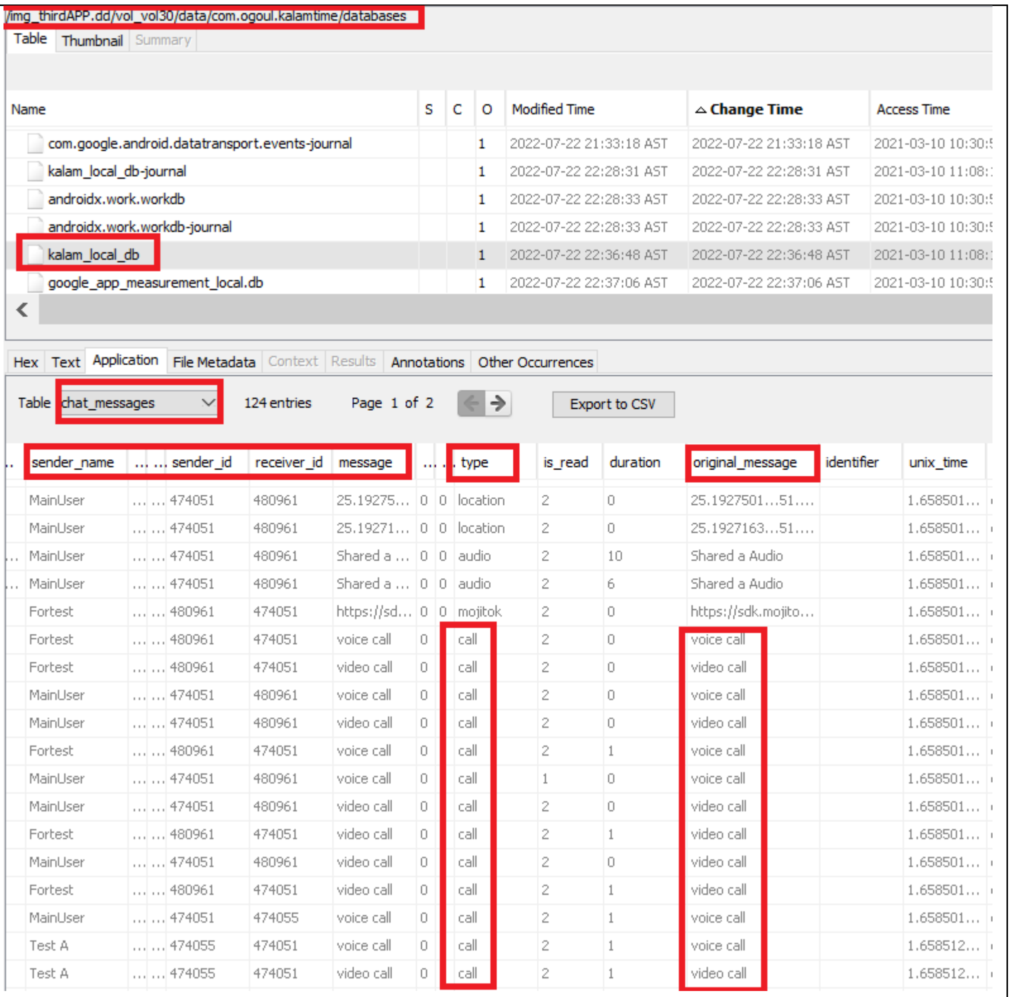
kalam_local_db
kalam_local_db-journal

Table chat_messages 195 entries Page 2 of 2

original_message	…	…	…	…	owner_name	forwarded_unix
Voice call		…	…			
Helloooooooooooo		…	…			
Helloooooooooooo		…	hi		Test A	1658518064.654
Ok		…	…		Test A	1658518087.306
Shared a Audio		…	…		Test A	1658512792.888
Shared a Audio		…	…		Test A	1658512872.615
Deleting from yo sode		…	…		Test A	1659173698.552
Ok		…	…		Test A	1659173699.936
Mine deketed		…	…		MainUser	1659173739.510
Ok		…	…		MainUser	1659173739.804

Table 5.38– Autopsy Test Result MDT-35, MDT-36, MDT-37, MDT-38

Test case id	MDT-54, MDT-55, MDT-56, MDT-58, MDT-59, MDT-60
Test case result	As expected
Test case analysis	Autopsy successfully extracted the caller and receiver’s phone number and timestamp.
Screenshots	

/img_thirdAPP.dd/vol_vol30/data/com.ogoul.kalamtime/databases

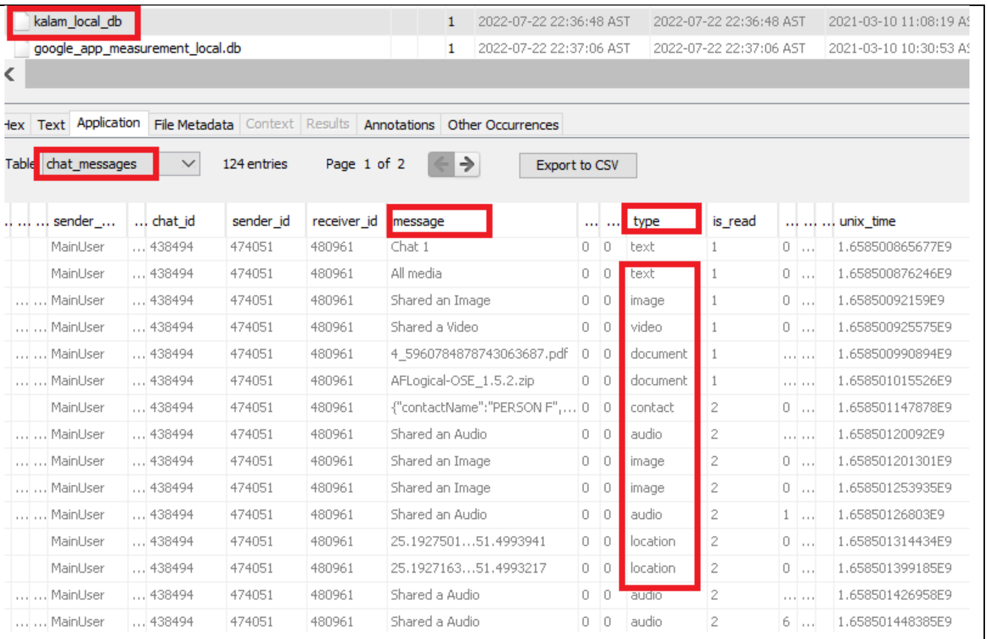
Name	S	C	O	Modified Time	Change Time	Access Time
com.google.android.datatransport.events-journal			1	2022-07-22 21:33:18 AST	2022-07-22 21:33:18 AST	2021-03-10 10:30:
kalam_local_db-journal			1	2022-07-22 22:28:31 AST	2022-07-22 22:28:31 AST	2021-03-10 11:08:
androidx.work.workdb			1	2022-07-22 22:28:33 AST	2022-07-22 22:28:33 AST	2021-03-10 10:30:
androidx.work.workdb-journal			1	2022-07-22 22:28:33 AST	2022-07-22 22:28:33 AST	2021-03-10 10:30:
kalam_local_db			1	2022-07-22 22:36:48 AST	2022-07-22 22:36:48 AST	2021-03-10 11:08:
google_app_measurement_local.db			1	2022-07-22 22:37:06 AST	2022-07-22 22:37:06 AST	2021-03-10 10:30:

Table chat_messages 124 entries Page 1 of 2

..	sender_name	...	...	sender_id	receiver_id	message	...	...	type	is_read	duration	original_message	identifier	unix_time
	MainUser	...	...	474051	480961	25.19275...	0	0	location	2	0	25.1927501...51....		1.658501...
	MainUser	...	...	474051	480961	25.19271...	0	0	location	2	0	25.1927163...51....		1.658501...
..	MainUser	...	...	474051	480961	Shared a ...	0	0	audio	2	10	Shared a Audio		1.658501...
..	MainUser	...	...	474051	480961	Shared a ...	0	0	audio	2	6	Shared a Audio		1.658501...
	Fortest	...	...	480961	474051	https://sd...	0	0	mojitok	2	0	https://sdk.mojito...		1.658501...
	Fortest	...	...	480961	474051	voice call	0		call	2	0	voice call		1.658501...
	Fortest	...	...	480961	474051	video call	0		call	2	0	video call		1.658501...
	MainUser	...	...	474051	480961	voice call	0		call	2	0	voice call		1.658501...
	MainUser	...	...	474051	480961	video call	0		call	2	0	video call		1.658501...
	Fortest	...	...	480961	474051	voice call	0		call	2	1	voice call		1.658501...
	MainUser	...	...	474051	480961	voice call	0		call	1	0	voice call		1.658501...
	MainUser	...	...	474051	480961	video call	0		call	2	0	video call		1.658501...
	Fortest	...	...	480961	474051	video call	0		call	2	1	video call		1.658501...
	MainUser	...	...	474051	480961	video call	0		call	2	0	video call		1.658501...
	Fortest	...	...	480961	474051	video call	0		call	2	1	video call		1.658501...
	MainUser	...	...	474051	474055	voice call	0		call	2	1	voice call		1.658501...
	Test A	...	...	474055	474051	voice call	0		call	2	1	voice call		1.658512...
	Test A	...	...	474055	474051	video call	0		call	2	1	video call		1.658512...

Table 5.39– Autopsy Test Result MDT-54, MDT-55, MDT-56, MDT-58, MDT-59, MDT-60

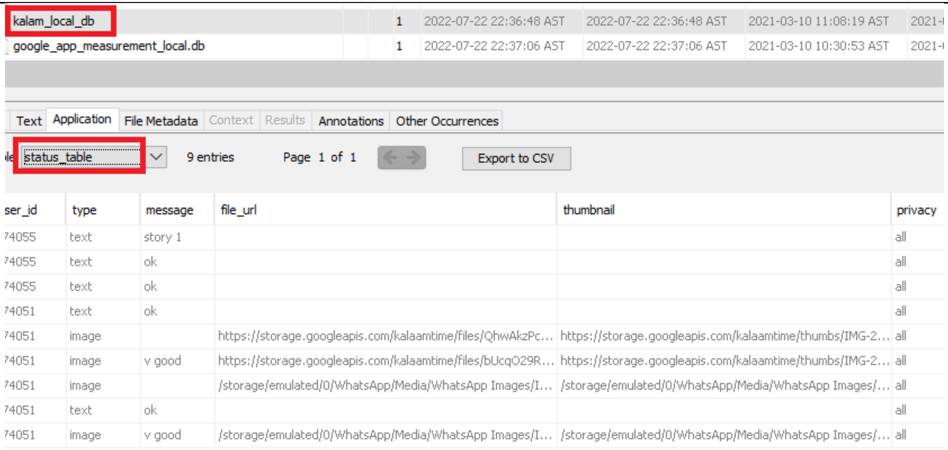
Test case id	MDT-62, MDT-63, MDT-64, MDT-65, MDT-97, MDT-98, MDT-99, MDT-100
Test case result	As expected
Test case analysis	Autopsy successfully found the sender and receiver of a media file, along with its content and type.
Screenshots	-

kalam_local_db	1	2022-07-22 22:36:48 AST	2022-07-22 22:36:48 AST	2021-03-10 11:08:19 A
google_app_measurement_local.db	1	2022-07-22 22:37:06 AST	2022-07-22 22:37:06 AST	2021-03-10 10:30:53 A

..	...	...	sender_...	...	chat_id	sender_id	receiver_id	message	...	...	type	is_read	...	...	...	unix_time
			MainUser	...	438494	474051	480961	Chat 1	0	0	text	1	0	...		1.658500865677E9
			MainUser	...	438494	474051	480961	All media	0	0	text	1	0	...		1.658500876246E9
	...	...	MainUser	...	438494	474051	480961	Shared an Image	0	0	image	1	0	...		1.65850092159E9
	...	...	MainUser	...	438494	474051	480961	Shared a Video	0	0	video	1	0	...		1.658500925575E9
	...	...	MainUser	...	438494	474051	480961	4_5960784878743063687.pdf	0	0	document	1	...	...		1.658500990894E9
	...	...	MainUser	...	438494	474051	480961	AFLogical-OSE_1.5.2.zip	0	0	document	1	...	...		1.658501015526E9
			MainUser	...	438494	474051	480961	{"contactName":"PERSON F",...	0	0	contact	2	0	...		1.658501147878E9
	...	...	MainUser	...	438494	474051	480961	Shared an Audio	0	0	audio	2	...	...		1.65850120092E9
	...	...	MainUser	...	438494	474051	480961	Shared an Image	0	0	image	2	0	...		1.658501201301E9
	...	...	MainUser	...	438494	474051	480961	Shared an Image	0	0	image	2	0	...		1.658501253935E9
	...	...	MainUser	...	438494	474051	480961	Shared an Audio	0	0	audio	2	1	...		1.65850126803E9
			MainUser	...	438494	474051	480961	25.1927501...51.4993941	0	0	location	2	0	...		1.658501314434E9
			MainUser	...	438494	474051	480961	25.1927163...51.4993217	0	0	location	2	0	...		1.658501399185E9
	...	...	MainUser	...	438494	474051	480961	Shared a Audio	0	0	audio	2	...	...		1.658501426958E9
	...	...	MainUser	...	438494	474051	480961	Shared a Audio	0	0	audio	2	6	...		1.658501448385E9

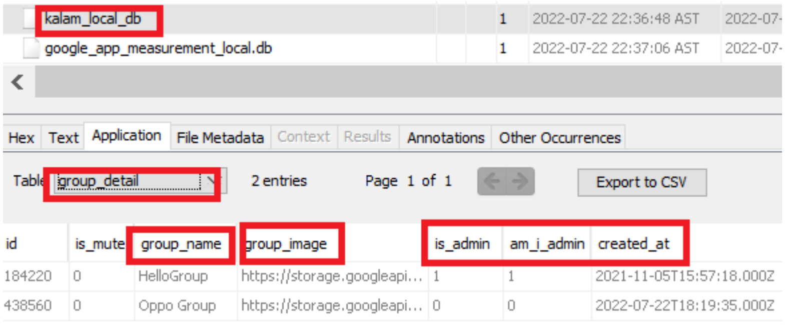
Table 5.40– Autopsy Test Result MDT-62, MDT-63, MDT-64, MDT-65, MDT-97, MDT-98, MDT-99, MDT-100

Test case id	MDT-68, MDT-69
Test case result	As expected
Test case analysis	Autopsy successfully found the type and content of an uploaded status.
Screenshots	

kalam_local_db	1	2022-07-22 22:36:48 AST	2022-07-22 22:36:48 AST	2021-03-10 11:08:19 AST	2021-
google_app_measurement_local.db	1	2022-07-22 22:37:06 AST	2022-07-22 22:37:06 AST	2021-03-10 10:30:53 AST	2021-

ser_id	type	message	file_url	thumbnail	privacy
74055	text	story 1			all
74055	text	ok			all
74055	text	ok			all
74051	text	ok			all
74051	image		https://storage.googleapis.com/kalaamtime/files/QhwAkzPc...	https://storage.googleapis.com/kalaamtime/thumbs/IMG-2...	all
74051	image	v good	https://storage.googleapis.com/kalaamtime/files/bUcqO29R...	https://storage.googleapis.com/kalaamtime/thumbs/IMG-2...	all
74051	image		/storage/emulated/0/WhatsApp/Media/WhatsApp Images/I...	/storage/emulated/0/WhatsApp/Media/WhatsApp Images/...	all
74051	text	ok			all
74051	image	v good	/storage/emulated/0/WhatsApp/Media/WhatsApp Images/I...	/storage/emulated/0/WhatsApp/Media/WhatsApp Images/...	all

Table 5.41– Autopsy Test Result MDT-68, MDT-69

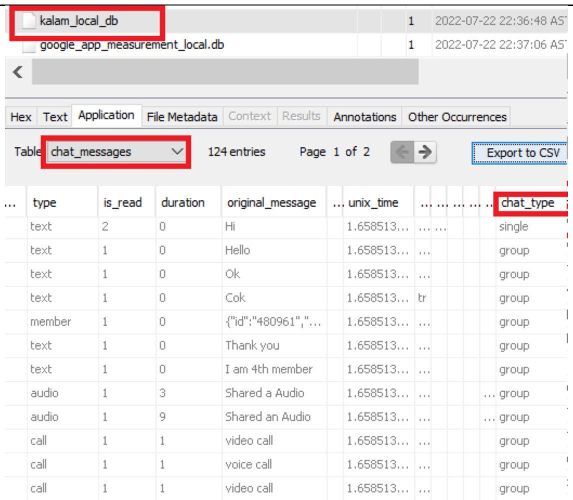
Test case id	MDT-75, MDT-76
Test case result	As expected
Test case analysis	Autopsy successfully found the group creation’s time and it’s admin’s name.
Screenshots	

kalam_local_db		1	2022-07-22 22:36:48 AST	2022-07-
google_app_measurement_local.db		1	2022-07-22 22:37:06 AST	2022-07-

Table group_detail 2 entries Page 1 of 1

id	is_mute	group_name	group_image	is_admin	am_i_admin	created_at
184220	0	HelloGroup	https://storage.googleapi…	1	1	2021-11-05T15:57:18.000Z
438560	0	Oppo Group	https://storage.googleapi…	0	0	2022-07-22T18:19:35.000Z

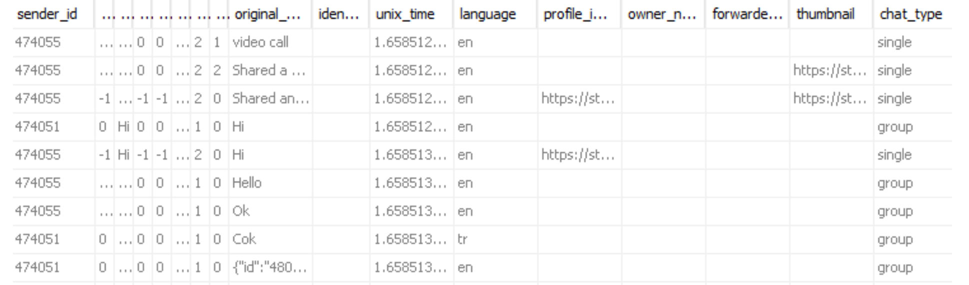
Table 5.42– Autopsy Test Result MDT-75, MDT-76

Test case id	MDT-78, MDT-79, MDT-80
Test case result	As expected
Test case analysis	Autopsy successfully found the sender’s phone number, timestamp. and chat content of a group’s message.
Screenshots	

kalam_local_db		1	2022-07-22 22:36:48 AS	
google_app_measurement_local.db		1	2022-07-22 22:37:06 AS	

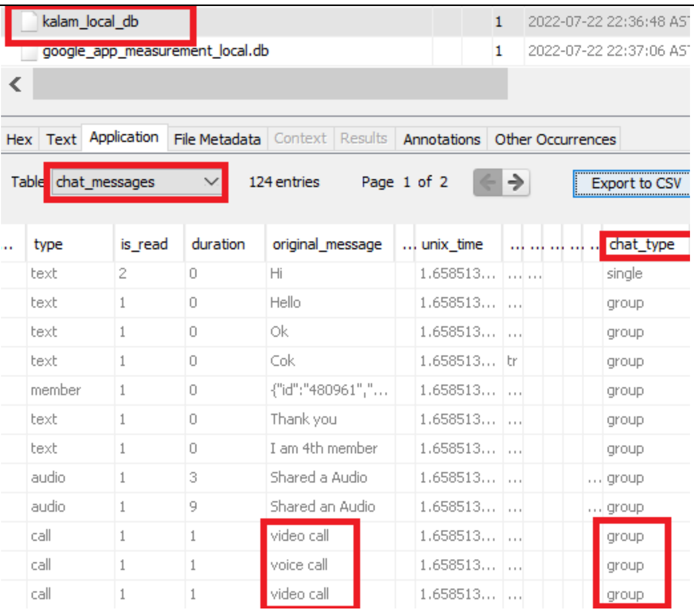
Table chat_messages 124 entries Page 1 of 2

…	type	is_read	duration	original_message	…	unix_time	…	…	…	…	…	chat_type
	text	2	0	Hi		1.658513…	…	…				single
	text	1	0	Hello		1.658513…	…					group
	text	1	0	Ok		1.658513…	…					group
	text	1	0	Cok		1.658513…	tr					group
	member	1	0	{"id":"480961","…		1.658513…	…					group
	text	1	0	Thank you		1.658513…	…					group
	text	1	0	I am 4th member		1.658513…	…					group
	audio	1	3	Shared a Audio		1.658513…	…				…	group
	audio	1	9	Shared an Audio		1.658513…	…				…	group
	call	1	1	video call		1.658513…	…					group
	call	1	1	voice call		1.658513…	…					group
	call	1	1	video call		1.658513…	…					group

sender_id	…	…	…	…	…	…	…	original_…	iden…	unix_time	language	profile_i…	owner_n…	forwarde…	thumbnail	chat_type
474055	…	…	0	0	…	2	1	video call		1.658512…	en					single
474055	…	…	0	0	…	2	2	Shared a …		1.658512…	en				https://st…	single
474055	-1	…	-1	-1	…	2	0	Shared an…		1.658512…	en	https://st…			https://st…	single
474051	0	Hi	0	0	…	1	0	Hi		1.658512…	en					group
474055	-1	Hi	-1	-1	…	2	0	Hi		1.658513…	en	https://st…				single
474055	…	…	0	0	…	1	0	Hello		1.658513…	en					group
474055	…	…	0	0	…	1	0	Ok		1.658513…	en					group
474051	0	…	0	0	…	1	0	Cok		1.658513…	tr					group
474051	0	…	0	0	…	1	0	{"id":"480…		1.658513…	en					group

Table 5.43– Autopsy Test Result MDT-78, MDT-79, MDT-80

Test case id	MDT-89, MDT-91, MDT-92, MDT-93, MDT-95, MDT-96
Test case result	As expected.
Test case analysis	Autopsy successfully found a caller’s phone number of a group voice call and video call, as well as timestamp and duration.
Screenshots	

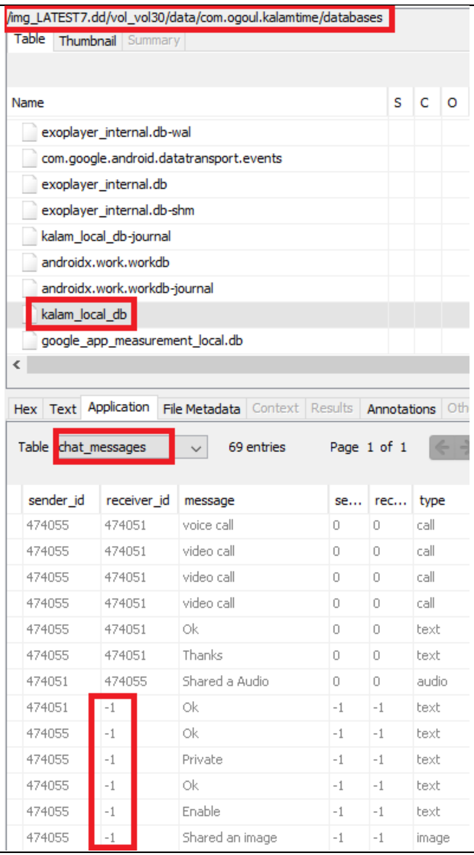
kalam_local_db		1	2022-07-22 22:36:48 AS
google_app_measurement_local.db		1	2022-07-22 22:37:06 AS

Table chat_messages 124 entries Page 1 of 2

..	type	is_read	duration	original_message	…	unix_time	…	…	…	…	..	chat_type
	text	2	0	Hi		1.658513…	…	…				single
	text	1	0	Hello		1.658513…	…					group
	text	1	0	Ok		1.658513…	…					group
	text	1	0	Cok		1.658513…	tr					group
	member	1	0	{"id":"480961","…		1.658513…	…					group
	text	1	0	Thank you		1.658513…	…					group
	text	1	0	I am 4th member		1.658513…	…					group
	audio	1	3	Shared a Audio		1.658513…	…				…	group
	audio	1	9	Shared an Audio		1.658513…	…				…	group
	call	1	1	video call		1.658513…	…					group
	call	1	1	voice call		1.658513…	…					group
	call	1	1	video call		1.658513…	…					group

Table 5.44– Autopsy Test Result MDT-89, MDT-91, MDT-92, MDT-93, MDT-95, MDT-96

Test case id	MDT-111, MDT-113, MDT-114
Test case result	As expected.
Test case analysis	Autopsy successfully found a secret message’s sender, timestamp, and chat content.

Screenshots	

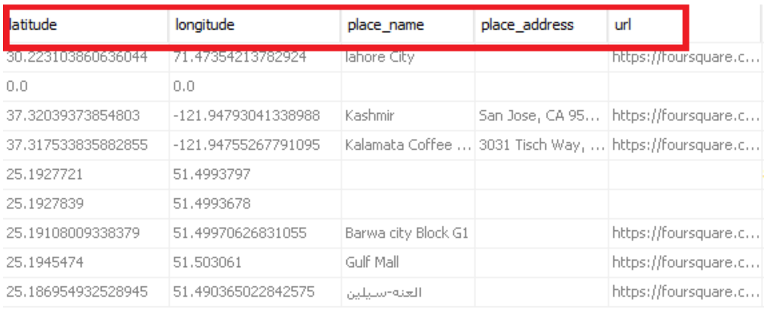
/img_LATEST7.dd/vol_vol30/data/com.ogoul.kalamtime/databases

Name	S	C	O
exoplayer_internal.db-wal			
com.google.android.datatransport.events			
exoplayer_internal.db			
exoplayer_internal.db-shm			
kalam_local_db-journal			
androidx.work.workdb			
androidx.work.workdb-journal			
kalam_local_db			
google_app_measurement_local.db			

Table chat_messages 69 entries Page 1 of 1

sender_id	receiver_id	message	se…	rec…	type
474055	474051	voice call	0	0	call
474055	474051	video call	0	0	call
474055	474051	video call	0	0	call
474055	474051	video call	0	0	call
474055	474051	Ok	0	0	text
474055	474051	Thanks	0	0	text
474051	474055	Shared a Audio	0	0	audio
474051	-1	Ok	-1	-1	text
474055	-1	Ok	-1	-1	text
474055	-1	Private	-1	-1	text
474055	-1	Ok	-1	-1	text
474055	-1	Enable	-1	-1	text
474055	-1	Shared an image	-1	-1	image

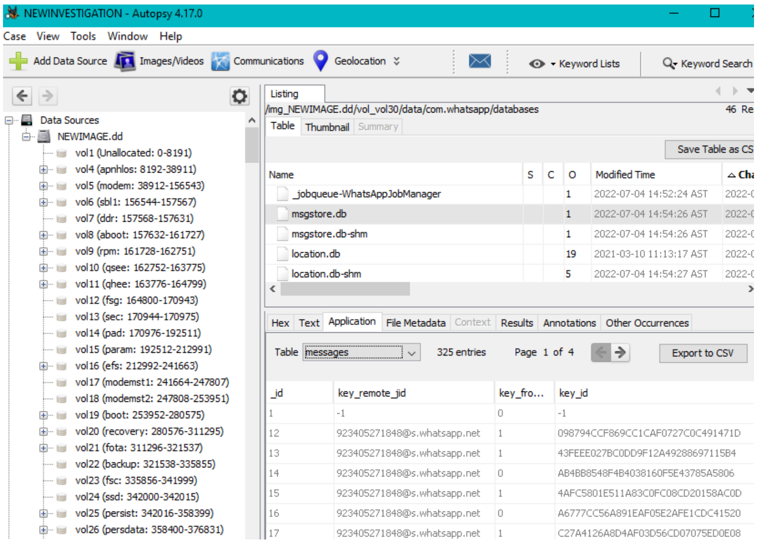
Table 5.45– Autopsy Test Result MDT-111, MDT-113, MDT-114

Test case id	MDT-120
Test case result	As expected.
Test case analysis	Autopsy was able to extract geolocation data present in social media chat messages.
Screenshots	

latitude	longitude	place_name	place_address	url
30.223103860636044	71.47354213782924	lahore City		https://foursquare.c…
0.0	0.0			
37.32039373854803	-121.94793041338988	Kashmir	San Jose, CA 95…	https://foursquare.c…
37.317533835882855	-121.94755267791095	Kalamata Coffee …	3031 Tisch Way, …	https://foursquare.c…
25.1927721	51.4993797			
25.1927839	51.4993678			
25.19108009338379	51.49970626831055	Barwa city Block G1		https://foursquare.c…
25.1945474	51.503061	Gulf Mall		https://foursquare.c…
25.186954932528945	51.490365022842575	العنه-سيلين		https://foursquare.c…

Table 5.46– Autopsy Test Result MDT-120

Test case id	MDT-121
Test case result	As expected
Test case analysis	Autopsy successfully presented the text with the correct character

	glyphs.
Screenshots	

NEWINVESTIGATION - Autopsy 4.17.0

Data Sources
- NEWIMAGE.dd
  - vol1 (Unallocated: 0-8191)
  - vol4 (apnhlos: 8192-38911)
  - vol5 (modem: 38912-156543)
  - vol6 (sbl1: 156544-157567)
  - vol7 (ddr: 157568-157631)
  - vol8 (aboot: 157632-161727)
  - vol9 (rpm: 161728-162751)
  - vol10 (qsee: 162752-163775)
  - vol11 (qhee: 163776-164799)
  - vol12 (fsg: 164800-170943)
  - vol13 (sec: 170944-170975)
  - vol14 (pad: 170976-192511)
  - vol15 (param: 192512-212991)
  - vol16 (efs: 212992-241663)
  - vol17 (modemst1: 241664-247807)
  - vol18 (modemst2: 247808-253951)
  - vol19 (boot: 253952-280575)
  - vol20 (recovery: 280576-311295)
  - vol21 (fota: 311296-321537)
  - vol22 (backup: 321538-335855)
  - vol23 (fsc: 335856-341999)
  - vol24 (ssd: 342000-342015)
  - vol25 (persist: 342016-358399)
  - vol26 (persdata: 358400-376831)

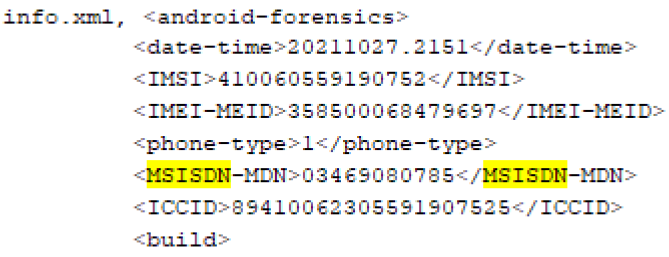
/img_NEWIMAGE.dd/vol_vol30/data/com.whatsapp/databases 46 Re

Name	S	C	O	Modified Time	Cha
_jobqueue-WhatsAppJobManager			1	2022-07-04 14:52:24 AST	2022-(
msgstore.db			1	2022-07-04 14:54:26 AST	2022-(
msgstore.db-shm			1	2022-07-04 14:54:26 AST	2022-(
location.db			19	2021-03-10 11:13:17 AST	2022-(
location.db-shm			5	2022-07-04 14:54:27 AST	2022-(

Table messages 325 entries Page 1 of 4

_id	key_remote_jid	key_fro...	key_id
1	-1	0	-1
12	923405271848@s.whatsapp.net	1	098794CCF869CC1CAF0727C0C491471D
13	923405271848@s.whatsapp.net	1	43FEEE027BC0DD9F12A49288697115B4
14	923405271848@s.whatsapp.net	0	AB4BB8548F4B4038160F5E43785A5806
15	923405271848@s.whatsapp.net	1	4AFC5801E511A83C0FC08CD20158AC0D
16	923405271848@s.whatsapp.net	0	A6777CC56A891EAF05E2AFE1CDC41520
17	923405271848@s.whatsapp.net	1	C27A4126A8D4AF03D56CD07075ED0E08

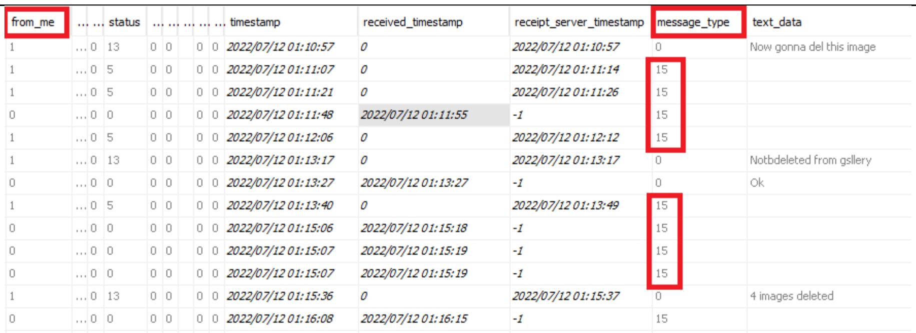
Table 5.47– Autopsy Test Result MDT-121

Test case id	MDT-132, MDT-133, MDT-134
Test case result	As expected.
Test case analysis	Autopsy successfully presented the ICCID, IMSI and MSISDN from the image file.
Screenshots	

```
info.xml, <android-forensics>
         <date-time>20211027.2151</date-time>
         <IMSI>410060559190752</IMSI>
         <IMEI-MEID>358500068479697</IMEI-MEID>
         <phone-type>1</phone-type>
         <MSISDN-MDN>03469080785</MSISDN-MDN>
         <ICCID>89410062305591907525</ICCID>
         <build>
```

Table 5.48– Autopsy Test Result MDT-132, MDT-133, MDT-134

Test case id	MDT-140
Test case result	Not checked
Test case analysis	Traces of the deleted data artifacts were found, but deleted content was not recovered by Autopsy.
Screenshots	



from_me	…	…	status	…	…	…	…	…	timestamp	received_timestamp	receipt_server_timestamp	message_type	text_data
1	…	0	13	0	0		0	0	2022/07/12 01:10:57	0	2022/07/12 01:10:57	0	Now gonna del this image
1	…	0	5	0	0		0	0	2022/07/12 01:11:07	0	2022/07/12 01:11:14	15	
1	…	0	5	0	0		0	0	2022/07/12 01:11:21	0	2022/07/12 01:11:26	15	
0	…	0	0	0	0		0	0	2022/07/12 01:11:48	2022/07/12 01:11:55	-1	15	
1	…	0	5	0	0		0	0	2022/07/12 01:12:06	0	2022/07/12 01:12:12	15	
1	…	0	13	0	0		0	0	2022/07/12 01:13:17	0	2022/07/12 01:13:17	0	Notbdeleted from gsllery
0	…	0	0	0	0		0	0	2022/07/12 01:13:27	2022/07/12 01:13:27	-1	0	Ok
1	…	0	5	0	0		0	0	2022/07/12 01:13:40	0	2022/07/12 01:13:49	15	
0	…	0	0	0	0		0	0	2022/07/12 01:15:06	2022/07/12 01:15:18	-1	15	
0	…	0	0	0	0		0	0	2022/07/12 01:15:07	2022/07/12 01:15:19	-1	15	
0	…	0	0	0	0		0	0	2022/07/12 01:15:07	2022/07/12 01:15:19	-1	15	
1	…	0	13	0	0		0	0	2022/07/12 01:15:36	0	2022/07/12 01:15:37	0	4 images deleted
0	…	0	0	0	0		0	0	2022/07/12 01:16:08	2022/07/12 01:16:15	-1	15	

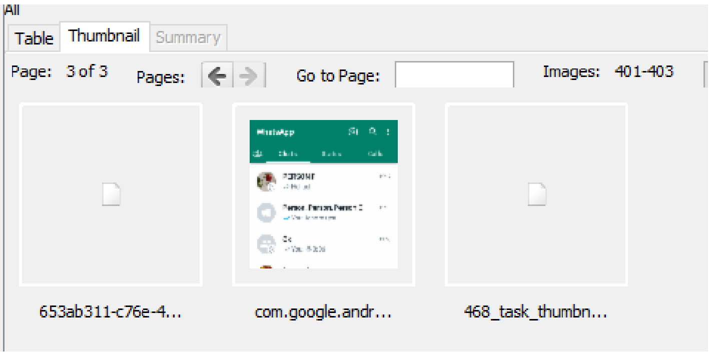
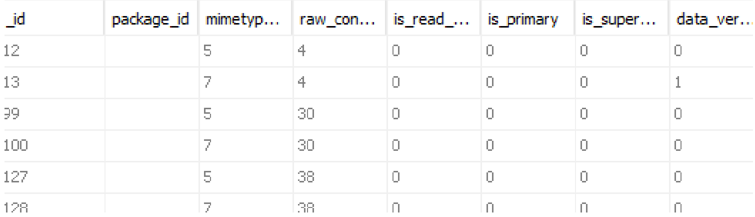


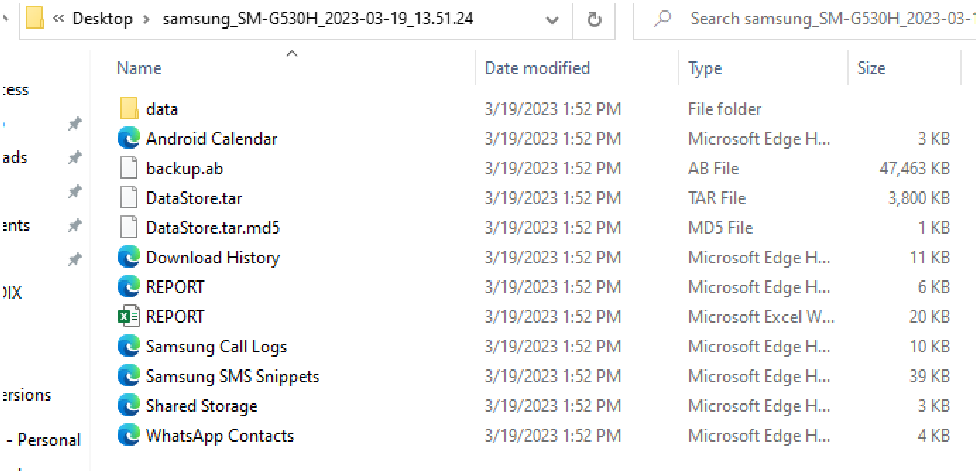
Table 5.48– Autopsy Test Result MDT-140

Test case id	MDT-141
Test case result	As expected.
Test case analysis	Autopsy database viewer successfully displayed the numeric values.
Screenshots	

_id	package_id	mimetyp...	raw_con...	is_read_...	is_primary	is_super...	data_ver..
12		5	4	0	0	0	0
13		7	4	0	0	0	1
39		5	30	0	0	0	0
100		7	30	0	0	0	0
127		5	38	0	0	0	0
128		7	38	0	0	0	0

Table 5.49– Autopsy Test Result MDT-141

5.3.2 Andriller Test Results Report

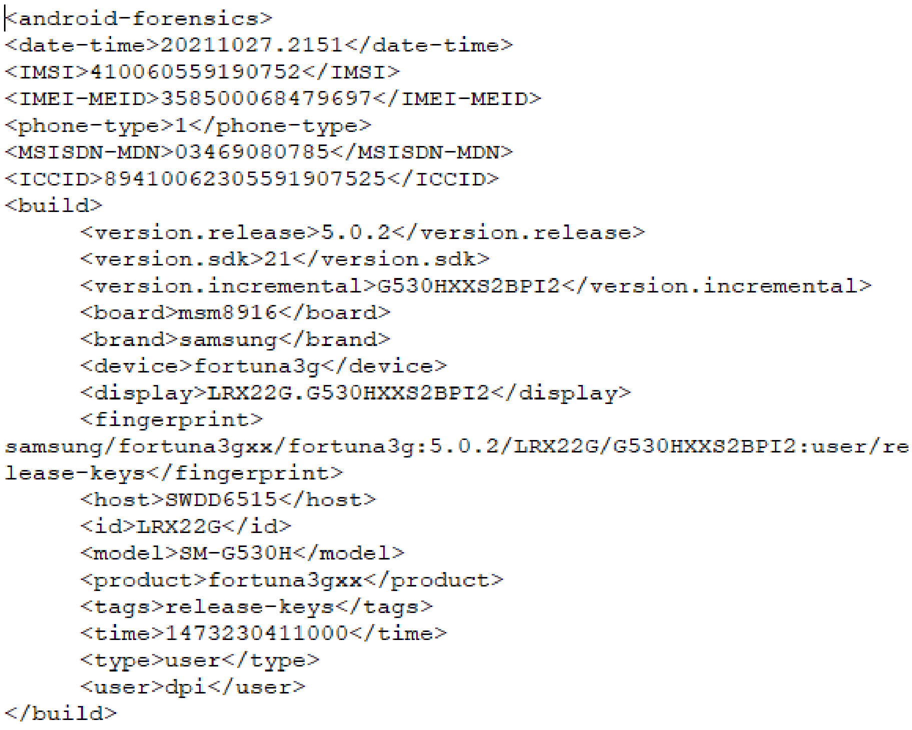


« Desktop › samsung_SM-G530H_2023-03-19_13.51.24

Search samsung_SM-G530H_2023-03-

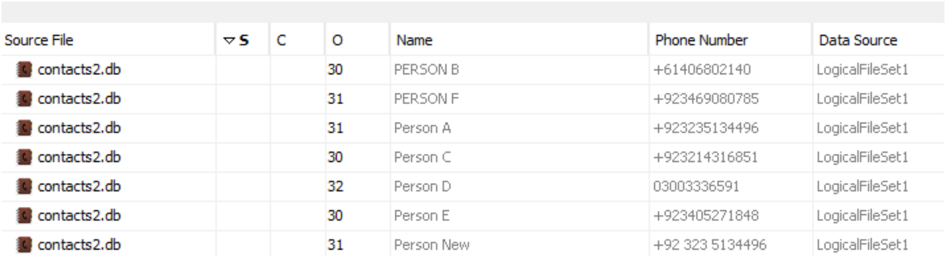
Name	Date modified	Type	Size
data	3/19/2023 1:52 PM	File folder	
Android Calendar	3/19/2023 1:52 PM	Microsoft Edge H...	3 KB
backup.ab	3/19/2023 1:52 PM	AB File	47,463 KB
DataStore.tar	3/19/2023 1:52 PM	TAR File	3,800 KB
DataStore.tar.md5	3/19/2023 1:52 PM	MD5 File	1 KB
Download History	3/19/2023 1:52 PM	Microsoft Edge H...	11 KB
REPORT	3/19/2023 1:52 PM	Microsoft Edge H...	6 KB
REPORT	3/19/2023 1:52 PM	Microsoft Excel W...	20 KB
Samsung Call Logs	3/19/2023 1:52 PM	Microsoft Edge H...	10 KB
Samsung SMS Snippets	3/19/2023 1:52 PM	Microsoft Edge H...	39 KB
Shared Storage	3/19/2023 1:52 PM	Microsoft Edge H...	3 KB
WhatsApp Contacts	3/19/2023 1:52 PM	Microsoft Edge H...	4 KB

Fig 5.3 Andriller overall extraction results

Test case id	MDT-02
Test case result	As expected.
Test case analysis	Andriller was able to show the equipment information.
Screenshots	

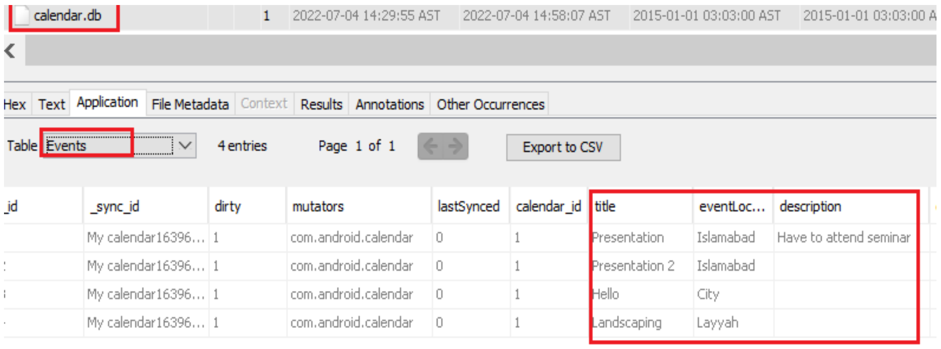
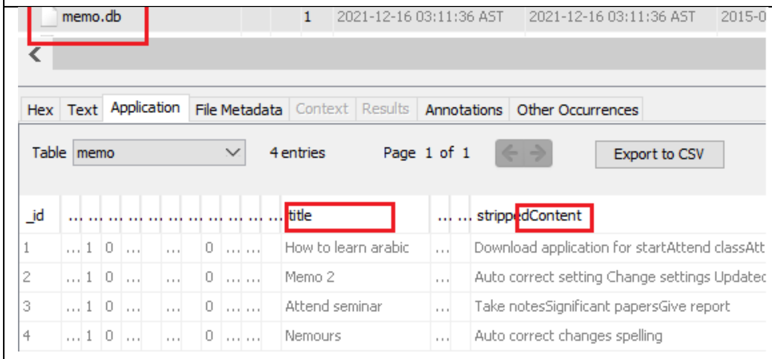
```
<android-forensics>
<date-time>20211027.2151</date-time>
<IMSI>410060559190752</IMSI>
<IMEI-MEID>358500068479697</IMEI-MEID>
<phone-type>1</phone-type>
<MSISDN-MDN>03469080785</MSISDN-MDN>
<ICCID>8941006230559l907525</ICCID>
<build>
      <version.release>5.0.2</version.release>
      <version.sdk>21</version.sdk>
      <version.incremental>G530HXXS2BPI2</version.incremental>
      <board>msm8916</board>
      <brand>samsung</brand>
      <device>fortuna3g</device>
      <display>LRX22G.G530HXXS2BPI2</display>
      <fingerprint>
samsung/fortuna3gxx/fortuna3g:5.0.2/LRX22G/G530HXXS2BPI2:user/re
lease-keys</fingerprint>
      <host>SWDD6515</host>
      <id>LRX22G</id>
      <model>SM-G530H</model>
      <product>fortuna3gxx</product>
      <tags>release-keys</tags>
      <time>1473230411000</time>
      <type>user</type>
      <user>dpi</user>
</build>
```

Table 5.50– Andriller Test Result MDT-02

Test case id	MDT-03
Test case result	Successful in combination with the Autopsy database viewer.
Test case analysis	Andriller was able to show address book data.
Screenshots	

Source File	▿ S	C	O	Name	Phone Number	Data Source
contacts2.db			30	PERSON B	+61406802140	LogicalFileSet1
contacts2.db			31	PERSON F	+923469080785	LogicalFileSet1
contacts2.db			31	Person A	+923235134496	LogicalFileSet1
contacts2.db			30	Person C	+923214316851	LogicalFileSet1
contacts2.db			32	Person D	03003336591	LogicalFileSet1
contacts2.db			30	Person E	+923405271848	LogicalFileSet1
contacts2.db			31	Person New	+92 323 5134496	LogicalFileSet1

Table 5.50– Andriller Test Result MDT-03

Test case id	MDT-04
Test case result	Successful in combination with the Autopsy database viewer.
Test case analysis	Andriller was able to show the calendar and notes' information.
Screenshots	 

calendar.db	1	2022-07-04 14:29:55 AST	2022-07-04 14:58:07 AST	2015-01-01 03:03:00 AST	2015-01-01 03:03:00 A

Hex | Text | Application | File Metadata | Context | Results | Annotations | Other Occurrences

Table Events 4 entries Page 1 of 1 Export to CSV

_id	_sync_id	dirty	mutators	lastSynced	calendar_id	title	eventLoc...	description
	My calendar16396...	1	com.android.calendar	0	1	Presentation	Islamabad	Have to attend seminar
	My calendar16396...	1	com.android.calendar	0	1	Presentation 2	Islamabad	
	My calendar16396...	1	com.android.calendar	0	1	Hello	City	
	My calendar16396...	1	com.android.calendar	0	1	Landscaping	Layyah	

memo.db	1	2021-12-16 03:11:36 AST	2021-12-16 03:11:36 AST	2015-0

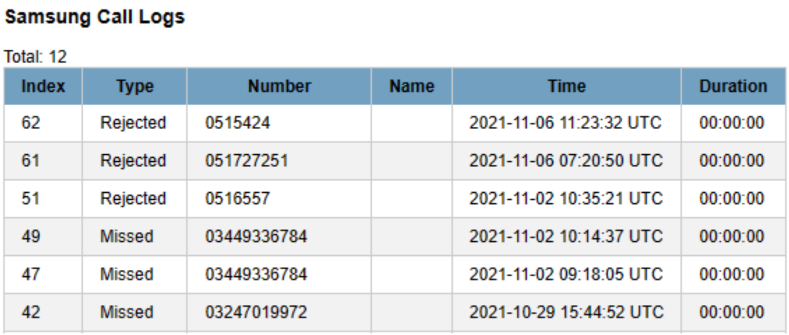
Hex | Text | Application | File Metadata | Context | Results | Annotations | Other Occurrences

Table memo 4 entries Page 1 of 1 Export to CSV

_id	…	…	…	…	…	…	…	…	…	…	…	title	…	…	strippedContent
1	…	1	0	…		…		0	…	…		How to learn arabic	…		Download application for startAttend classAtt
2	…	1	0	…		…		0	…	…		Memo 2	…		Auto correct setting Change settings Updatec
3	…	1	0	…		…		0	…	…		Attend seminar	…		Take notesSignificant papersGive report
4	…	1	0	…		…		0	…	…		Nemours	…		Auto correct changes spelling

Table 5.52– Andriller Test Result MDT-04

Test case id	MDT-05

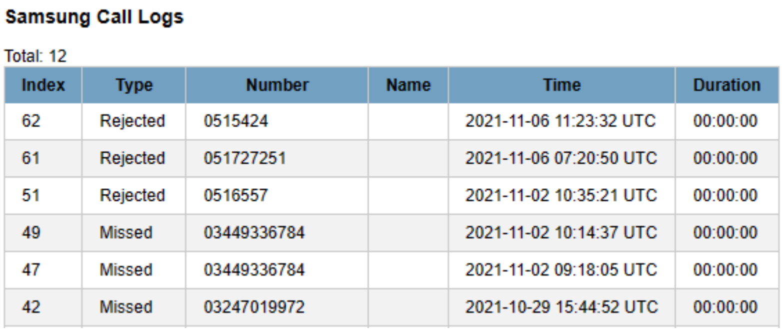
Test case result	As expected
Test case analysis	Andriller was able to show the incoming call data.
Screenshots	

Samsung Call Logs

Total: 12

Index	Type	Number	Name	Time	Duration
62	Rejected	0515424		2021-11-06 11:23:32 UTC	00:00:00
61	Rejected	051727251		2021-11-06 07:20:50 UTC	00:00:00
51	Rejected	0516557		2021-11-02 10:35:21 UTC	00:00:00
49	Missed	03449336784		2021-11-02 10:14:37 UTC	00:00:00
47	Missed	03449336784		2021-11-02 09:18:05 UTC	00:00:00
42	Missed	03247019972		2021-10-29 15:44:52 UTC	00:00:00

Table 5.53– Andriller Test Result MDT-05

Test case id	MDT-06, MDT-08
Test case result	As expected
Test case analysis	Andriller was able to show the outgoing call data.
Screenshots	

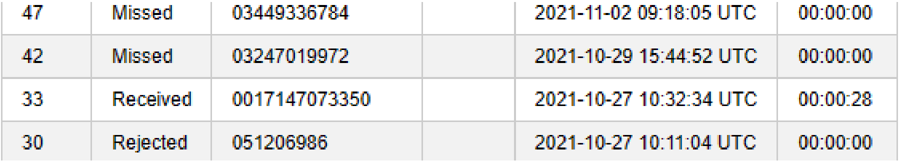
Samsung Call Logs

Total: 12

Index	Type	Number	Name	Time	Duration
62	Rejected	0515424		2021-11-06 11:23:32 UTC	00:00:00
61	Rejected	051727251		2021-11-06 07:20:50 UTC	00:00:00
51	Rejected	0516557		2021-11-02 10:35:21 UTC	00:00:00
49	Missed	03449336784		2021-11-02 10:14:37 UTC	00:00:00
47	Missed	03449336784		2021-11-02 09:18:05 UTC	00:00:00
42	Missed	03247019972		2021-10-29 15:44:52 UTC	00:00:00

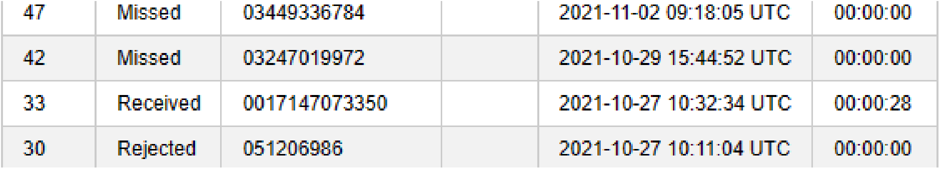
Table 5.54– Andriller Test Result MDT-06, MDT-08

Test case id	MDT-07
Test case result	As expected
Test case analysis	Andriller was able to show missed call data.

Screenshots	

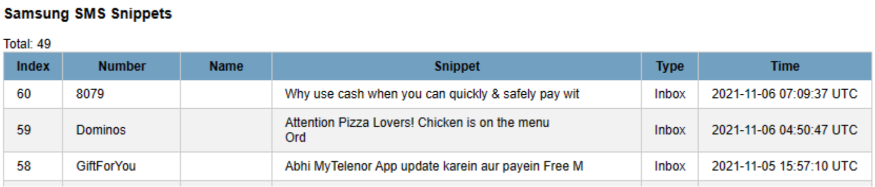
47	Missed	03449336784		2021-11-02 09:18:05 UTC	00:00:00
42	Missed	03247019972		2021-10-29 15:44:52 UTC	00:00:00
33	Received	0017147073350		2021-10-27 10:32:34 UTC	00:00:28
30	Rejected	051206986		2021-10-27 10:11:04 UTC	00:00:00

Table 5.55– Andriller Test Result MDT-07

Test case id	MDT-09
Test case result	As expected.
Test case analysis	Andriller was able to show the duration of calls.
Screenshots	

47	Missed	03449336784		2021-11-02 09:18:05 UTC	00:00:00
42	Missed	03247019972		2021-10-29 15:44:52 UTC	00:00:00
33	Received	0017147073350		2021-10-27 10:32:34 UTC	00:00:28
30	Rejected	051206986		2021-10-27 10:11:04 UTC	00:00:00

Table 5.56– Andriller Test Result MDT-09

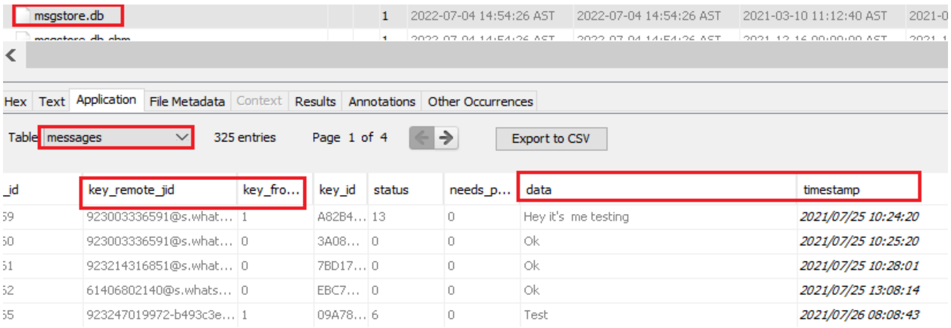
Test case id	MDT-10, MDT-13
Test case result	As expected.
Test case analysis	Andriller was able to show the local messages with time stamps.
Screenshots	

Samsung SMS Snippets

Total: 49

Index	Number	Name	Snippet	Type	Time
60	8079		Why use cash when you can quickly & safely pay wit	Inbox	2021-11-06 07:09:37 UTC
59	Dominos		Attention Pizza Lovers! Chicken is on the menu Ord	Inbox	2021-11-06 04:50:47 UTC
58	GiftForYou		Abhi MyTelenor App update karein aur payein Free M	Inbox	2021-11-05 15:57:10 UTC

Table 5.57– Andriller Test Result MDT-10, MDT-13

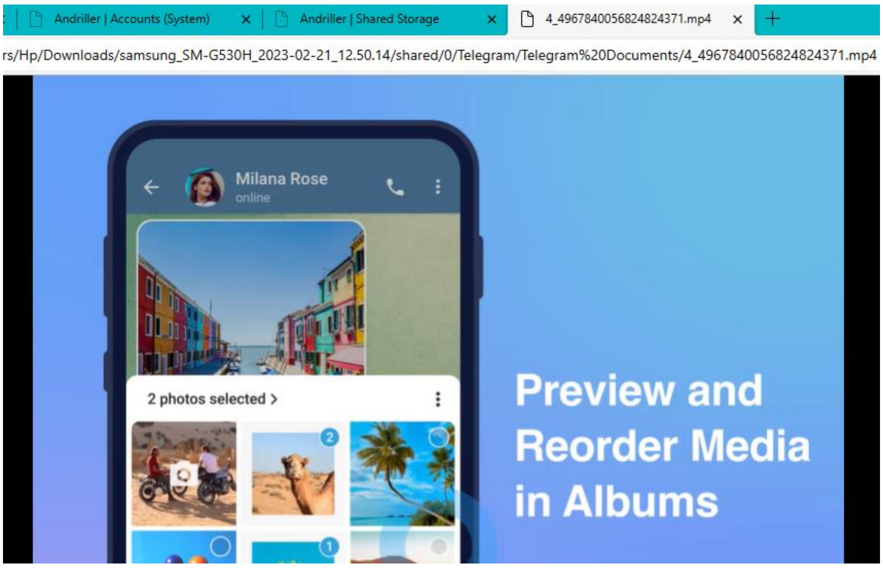
Test case id	MDT-12, MDT-15
Test case result	Successful in combination with the Autopsy database viewer.
Test case analysis	Andriller was able to show instant messages with time stamps.
Screenshots	

msgstore.db 1 2022-07-04 14:54:26 AST 2022-07-04 14:54:26 AST 2021-03-10 11:12:40 AST 2021-0

Table messages 325 entries Page 1 of 4

_id	key_remote_jid	key_fro...	key_id	status	needs_p...	data	timestamp
59	923003336591@s.what...	1	A82B4...	13	0	Hey it's me testing	*2021/07/25 10:24:20*
50	923003336591@s.what...	0	3A08...	0	0	Ok	*2021/07/25 10:25:20*
51	923214316851@s.what...	0	7BD17...	0	0	Ok	*2021/07/25 10:28:01*
52	61406802140@s.whats...	0	EBC7...	0	0	Ok	*2021/07/25 13:08:14*
55	923247019972-b493c3e...	1	09A78...	6	0	Test	*2021/07/26 08:08:43*

Table 5.58– Andriller Test Result MDT-12, MDT-15

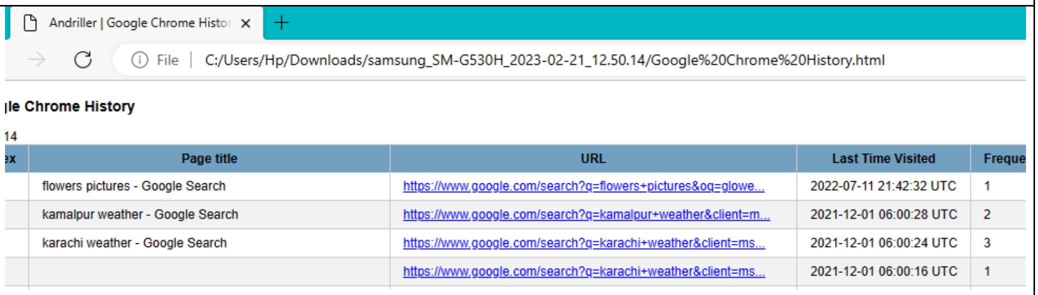
Test case id	MDT-17
Test case result	As expected.
Test case analysis	Andriller was able to show and play the video files.
Screenshots	

Andriller | Accounts (System)
Andriller | Shared Storage
4_4967840056824824371.mp4
Milana Rose
online
2 photos selected >
Preview and Reorder Media in Albums

rs/Hp/Downloads/samsung_SM-G530H_2023-02-21_12.50.14/shared/0/Telegram/Telegram%20Documents/4_4967840056824824371.mp4

Table 5.59– Andriller Test Result MDT-17

Test case id	MDT-20

Test case result	As expected
Test case analysis	Andriller was able to show the browsing history.
Screenshots	

Andriller | Google Chrome Histor

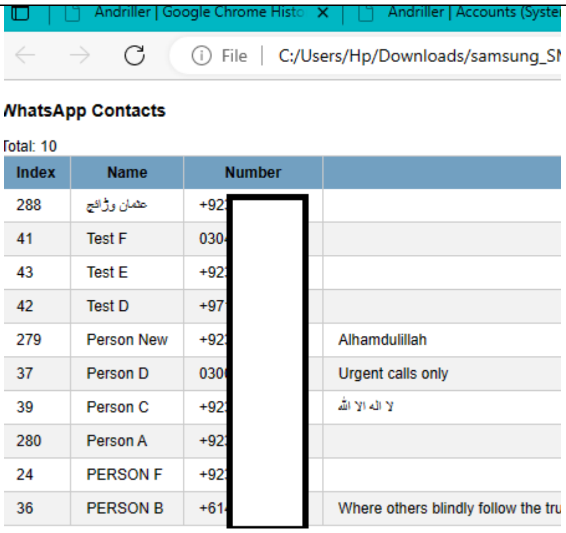
File | C:/Users/Hp/Downloads/samsung_SM-G530H_2023-02-21_12.50.14/Google%20Chrome%20History.html

ıle Chrome History

14

ex	Page title	URL	Last Time Visited	Freque
	flowers pictures - Google Search	https://www.google.com/search?q=flowers+pictures&oq=glowe...	2022-07-11 21:42:32 UTC	1
	kamalpur weather - Google Search	https://www.google.com/search?q=kamalpur+weather&client=m...	2021-12-01 06:00:28 UTC	2
	karachi weather - Google Search	https://www.google.com/search?q=karachi+weather&client=ms...	2021-12-01 06:00:24 UTC	3
		https://www.google.com/search?q=karachi+weather&client=ms...	2021-12-01 06:00:16 UTC	1

Table 5.60– Andriller Test Result MDT-20

Test case id	MDT-26, MDT-28
Test case result	As expected
Test case analysis	Andriller successfully presented the contact's name and phone number within WhatsApp.
Screenshots	

Andriller | Google Chrome Histo | Andriller | Accounts (Syste

File | C:/Users/Hp/Downloads/samsung_SI

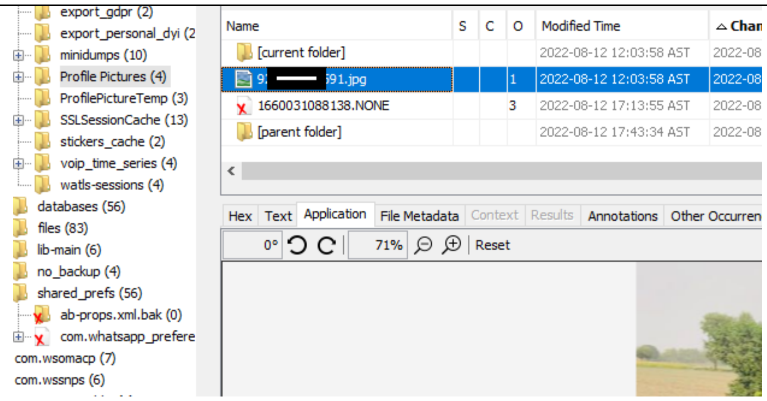
VhatsApp Contacts

Total: 10

Index	Name	Number	
288	عثمان وڑائچ	[redacted]	
41	Test F	[redacted]	
43	Test E	[redacted]	
42	Test D	[redacted]	
279	Person New	[redacted]	Alhamdulillah
37	Person D	[redacted]	Urgent calls only
39	Person C	[redacted]	لا اله الا الله
280	Person A	[redacted]	
24	PERSON F	[redacted]	
36	PERSON B	[redacted]	Where others blindly follow the tru

Table 5.61– Andriller Test Result MDT-26, MDT-28

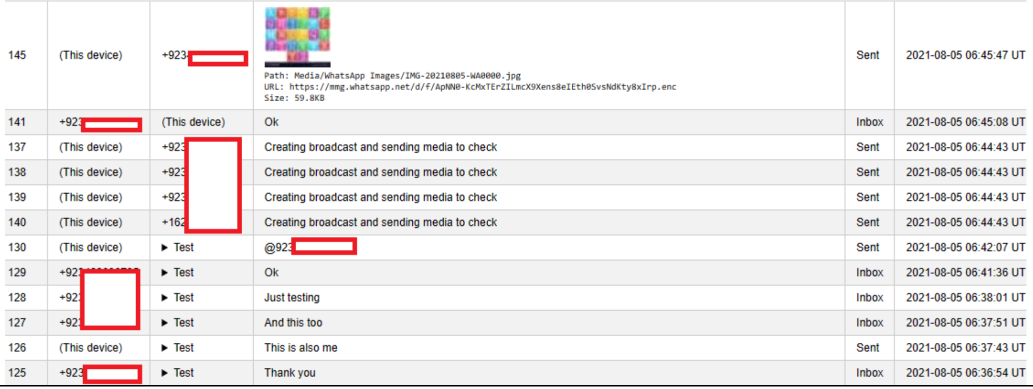
Test case id	MDT-27

Test case result	Successful in combination with the Autopsy database viewer.
Test case analysis	Andriller was able to present the profile picture of WhatsApp contacts.
Screenshots	

export_gdpr (2)
export_personal_dyi (2
minidumps (10)
Profile Pictures (4)
ProfilePictureTemp (3)
SSLSessionCache (13)
stickers_cache (2)
voip_time_series (4)
watls-sessions (4)
databases (56)
files (83)
lib-main (6)
no_backup (4)
shared_prefs (56)
ab-props.xml.bak (0)
com.whatsapp_prefere
com.wsomacp (7)
com.wssnps (6)

Name	S	C	O	Modified Time	△ Chan
[current folder]				2022-08-12 12:03:58 AST	2022-08
9[redacted]91.jpg			1	2022-08-12 12:03:58 AST	2022-08
1660031088138.NONE			3	2022-08-12 17:13:55 AST	2022-08
[parent folder]				2022-08-12 17:43:34 AST	2022-08

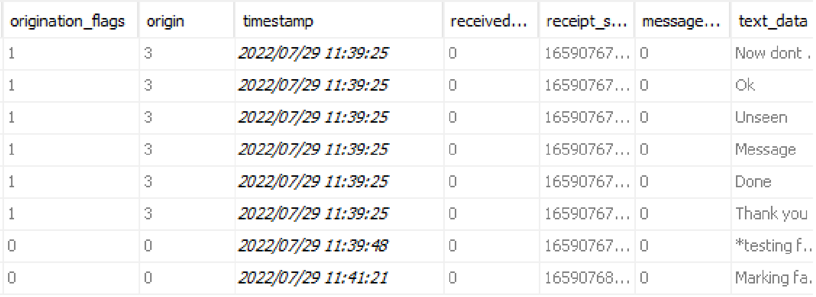
Table 5.62– Andriller Test Result MDT-27

Test case id	MDT-31, MDT-32, MDT-33, MDT-34, MDT-35, MDT-36, MDT-40, MDT-41, MDT-44, MDT-45, MDT-50, MDT-51, MDT-52, MDT-53, MDT-62, MDT-63, MDT-81, MDT-82, MDT-83, MDT-97, MDT-98, MDT-104, MDT-105, MDT-108
Test case result	As expected
Test case analysis	Andriller successfully extracted the sender and receiver's phone number, and also the timestamp and chat content of a chat message.
Screenshots	

145	(This device)	+923[redacted]	Path: Media/WhatsApp Images/IMG-20210805-WA0000.jpg URL: https://mmg.whatsapp.net/d/f/ApNN0-KcMxTErZILmcX9Xens8eIEth0SvsNdKty8xIrp.enc Size: 59.8KB	Sent	2021-08-05 06:45:47 UT
141	+923[redacted]	(This device)	Ok	Inbox	2021-08-05 06:45:08 UT
137	(This device)	+923[redacted]	Creating broadcast and sending media to check	Sent	2021-08-05 06:44:43 UT
138	(This device)	+923[redacted]	Creating broadcast and sending media to check	Sent	2021-08-05 06:44:43 UT
139	(This device)	+923[redacted]	Creating broadcast and sending media to check	Sent	2021-08-05 06:44:43 UT
140	(This device)	+162[redacted]	Creating broadcast and sending media to check	Sent	2021-08-05 06:44:43 UT
130	(This device)	▶ Test	@923[redacted]	Sent	2021-08-05 06:42:07 UT
129	+92[redacted]	▶ Test	Ok	Inbox	2021-08-05 06:41:36 UT
128	+92[redacted]	▶ Test	Just testing	Inbox	2021-08-05 06:38:01 UT
127	+92[redacted]	▶ Test	And this too	Inbox	2021-08-05 06:37:51 UT
126	(This device)	▶ Test	This is also me	Sent	2021-08-05 06:37:43 UT
125	+923[redacted]	▶ Test	Thank you	Inbox	2021-08-05 06:36:54 UT

Table 5.63– Andriller Test Result MDT-31, MDT-32, MDT-33, MDT-34, MDT-35, MDT-36, MDT-40, MDT-41, MDT-44, MDT-45, MDT-50, MDT-51, MDT-52, MDT-53, MDT-62, MDT-63, MDT-81, MDT-82, MDT-83, MDT-97, MDT-98, MDT-104, MDT-105, MDT-108

Test case id	MDT-37, MDT-38

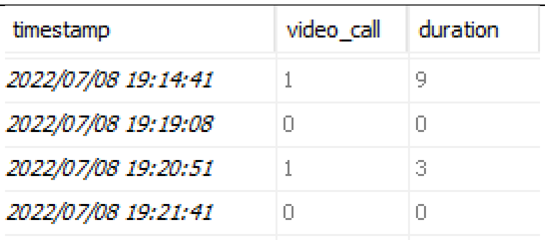
Test case result	Successful in combination with the Autopsy database viewer.
Test case analysis	Andriller successfully presented the timestamp and chat content of a forwarded message. The origination_flags column’s value is 1 in case of a forwarded message.
Screenshots	

origination_flags	origin	timestamp	received...	receipt_s...	message...	text_data
1	3	*2022/07/29 11:39:25*	0	16590767...	0	Now dont .
1	3	*2022/07/29 11:39:25*	0	16590767...	0	Ok
1	3	*2022/07/29 11:39:25*	0	16590767...	0	Unseen
1	3	*2022/07/29 11:39:25*	0	16590767...	0	Message
1	3	*2022/07/29 11:39:25*	0	16590767...	0	Done
1	3	*2022/07/29 11:39:25*	0	16590767...	0	Thank you
0	0	*2022/07/29 11:39:48*	0	16590767...	0	*testing f..
0	0	*2022/07/29 11:41:21*	0	16590768...	0	Marking fa.

Table 5.64– Andriller Test Result MDT-37, MDT-38

Test case id	MDT-39
Test case result	Not checked.
Test case analysis	Andriller was unable to extract the original author of a forwarded message.
Screenshots	-

Table 5.65– Andriller Test Result MDT-39

Test case id	MDT-60, MDT-61, MDT-95, MDT-96
Test case result	Successful in combination with the Autopsy database viewer.
Test case analysis	Andriller successfully presented the timestamp and duration of a video call.
Screenshots	

timestamp	video_call	duration
2022/07/08 19:14:41	1	9
2022/07/08 19:19:08	0	0
2022/07/08 19:20:51	1	3
2022/07/08 19:21:41	0	0

Table 5.66– Andriller Test Result MDT-60, MDT-61, MDT-95, MDT-96

Test case id	MDT-64, MDT-65, MDT-99, MDT-100, MDT-109, MDT-110

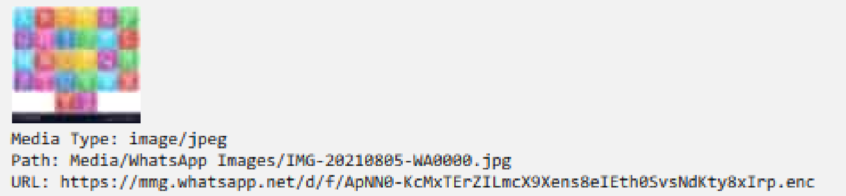
Test case result	As expected.
Test case analysis	Andriller successfully presented the content and type of a media file.
Screenshots	 Media Type: image/jpeg Path: Media/WhatsApp Images/IMG-20210805-WA0000.jpg URL: https://mmg.whatsapp.net/d/f/ApNN0-KcMxTErZILmcX9Xens8eIEth0SvsNdKty8xIrp.enc

Table 5.67– Andriller Test Result MDT-64, MDT-65, MDT-99, MDT-100, MDT-109, MDT-110

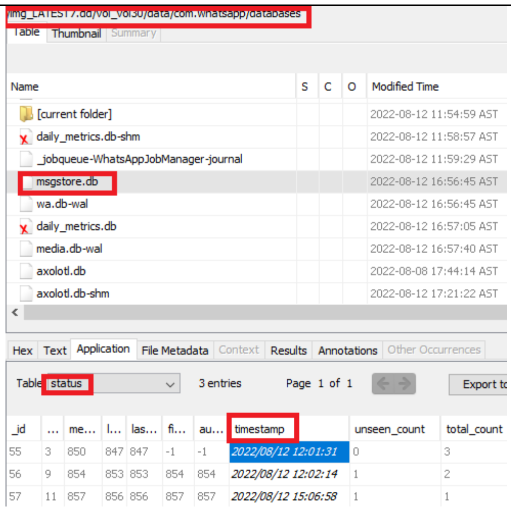
Test case id	MDT-67
Test case result	Successful in combination with the Autopsy database viewer.
Test case analysis	Andriller successfully presented the timestamp when a status was uploaded.
Screenshots	 /img_LATEST7.dd/vol_vol30/data/com.whatsapp/databases Name | S | C | O | Modified Time [current folder] | 2022-08-12 11:54:59 AST daily_metrics.db-shm | 2022-08-12 11:58:57 AST _jobqueue-WhatsAppJobManager-journal | 2022-08-12 11:59:29 AST msgstore.db | 2022-08-12 16:56:45 AST wa.db-wal | 2022-08-12 16:56:45 AST daily_metrics.db | 2022-08-12 16:57:05 AST media.db-wal | 2022-08-12 16:57:40 AST axolotl.db | 2022-08-08 17:44:14 AST axolotl.db-shm | 2022-08-12 17:21:22 AST Table status | 3 entries | Page 1 of 1 _id | ... | me... | l... | las... | fi... | au... | timestamp | unseen_count | total_count 55 | 3 | 850 | 847 | 847 | -1 | -1 | 2022/08/12 12:01:31 | 0 | 3 56 | 9 | 854 | 853 | 853 | 854 | 854 | 2022/08/12 12:02:14 | 1 | 2 57 | 11 | 857 | 856 | 856 | 857 | 857 | 2022/08/12 15:06:58 | 1 | 1

Table 5.68– Andriller Test Result MDT-67

Test case id	MDT-75
Test case result	Successful in combination with the Autopsy database viewer.
Test case analysis	Andriller successfully found the time when a group was created.

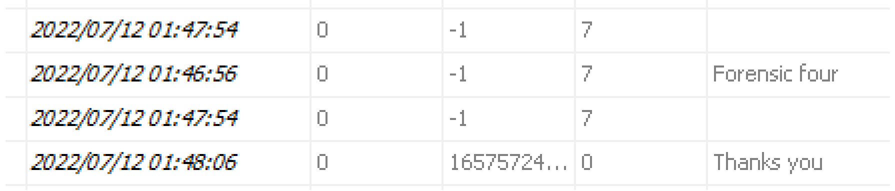
Screenshots	 2022/07/12 01:47:54 0 -1 7 2022/07/12 01:46:56 0 -1 7 Forensic four 2022/07/12 01:47:54 0 -1 7 2022/07/12 01:48:06 0 16575724… 0 Thanks you

Table 5.69– Andriller Test Result MDT-75

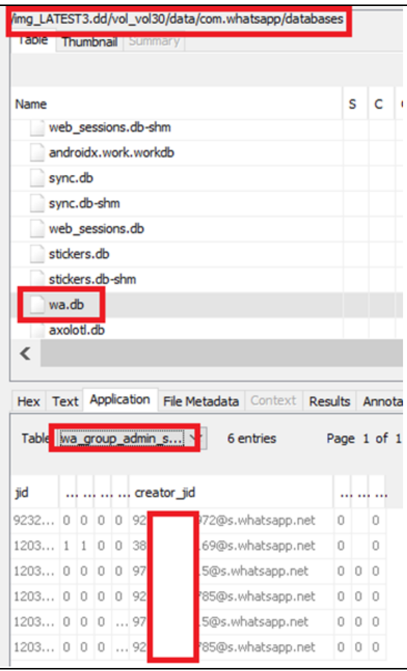
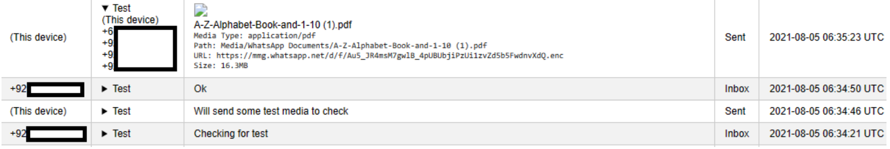
Test case id	MDT-76
Test case result	Successful in combination with the Autopsy database viewer.
Test case analysis	Andriller was able to extract a group admin’s phone number.
Screenshots	 /img_LATEST3.dd/vol_vol30/data/com.whatsapp/databases Table Thumbnail Summary Name S C web_sessions.db-shm androidx.work.workdb sync.db sync.db-shm web_sessions.db stickers.db stickers.db-shm wa.db axolotl.db Hex Text Application File Metadata Context Results Annota Table wa_group_admin_s... 6 entries Page 1 of 1 jid … … … … creator_jid … … … 9232… 0 0 0 0 92[redacted]72@s.whatsapp.net 0 0 1203… 1 1 0 0 38[redacted]69@s.whatsapp.net 0 0 1203… 0 0 0 0 97[redacted]5@s.whatsapp.net 0 0 0 1203… 0 0 0 0 92[redacted]85@s.whatsapp.net 0 0 0 1203… 0 0 0 … 97[redacted]5@s.whatsapp.net 0 0 0 1203… 0 0 0 … 92[redacted]85@s.whatsapp.net 0 0 0

Table 5.70– Andriller Test Result MDT-76

Test case id	MDT-77
Test case result	Not checked.
Test case analysis	Andriller was unable to extract the phone number of a group participant directly, phone numbers of active members could be extracted from the messages table.
Screenshots	-

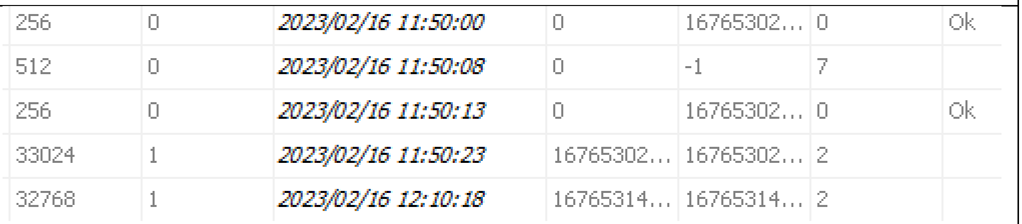
Table 5.71– Andriller Test Result MDT-77

Test case id	MDT-79, MDT-80
Test case	As expected.

result	
Test case analysis	Andriller successfully displayed the timestamp and content of a group's chat message.
Screenshots	

(This device)	▼ Test (This device) +6 +9 +9 +9 [redacted]	A-Z-Alphabet-Book-and-1-10 (1).pdf Media Type: application/pdf Path: Media/WhatsApp Documents/A-Z-Alphabet-Book-and-1-10 (1).pdf URL: https://mmg.whatsapp.net/d/f/Au5_JR4msM7gwlB_4pUBUbjiPzUi1zvZd5b5FwdnvXdQ.enc Size: 16.3MB	Sent	2021-08-05 06:35:23 UTC
+92 [redacted]	▶ Test	Ok	Inbox	2021-08-05 06:34:50 UTC
(This device)	▶ Test	Will send some test media to check	Sent	2021-08-05 06:34:46 UTC
+92 [redacted]	▶ Test	Checking for test	Inbox	2021-08-05 06:34:21 UTC

Table 5.72– Andriller Test Result MDT-79, MDT-80

Test case id	MDT-86, MDT-87
Test case result	Successful in combination with the Autopsy database viewer.
Test case analysis	Andriller successfully displayed the timestamp of a group's voice message.
Screenshots	

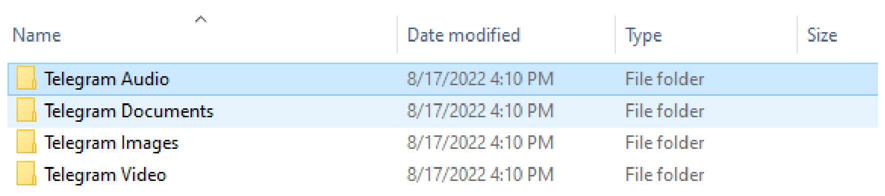
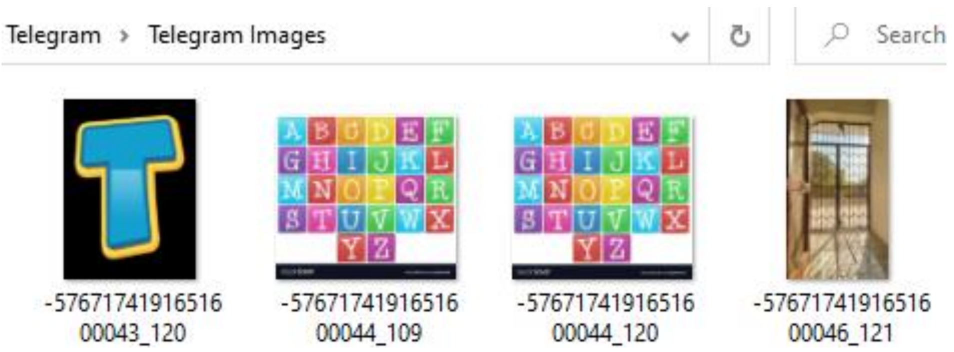
256	0	*2023/02/16 11:50:00*	0	16765302...	0	Ok
512	0	*2023/02/16 11:50:08*	0	-1	7	
256	0	*2023/02/16 11:50:13*	0	16765302...	0	Ok
33024	1	*2023/02/16 11:50:23*	16765302...	16765302...	2	
32768	1	*2023/02/16 12:10:18*	16765314...	16765314...	2	

Table 5.73– Andriller Test Result MDT-86, MDT-87

Test case id	MDT-102, MDT-103
Test case result	Not checked.
Test case analysis	Andriller was unable to display the creator and recipient of a broadcast.
Screenshots	-

Table 5.74–Andriller Test Result   MDT-102, MDT-103

Test case id	MDT-64, MDT-65, MDT-99, MDT-100, MDT-109, MDT-110
Test case result	As expected.

Test case analysis	Andriller was able to display the content and type of media files sent and received in simple chat messages, group chat messages, and broadcasted messages.
Screenshots	 

Name	Date modified	Type	Size
Telegram Audio	8/17/2022 4:10 PM	File folder	
Telegram Documents	8/17/2022 4:10 PM	File folder	
Telegram Images	8/17/2022 4:10 PM	File folder	
Telegram Video	8/17/2022 4:10 PM	File folder	

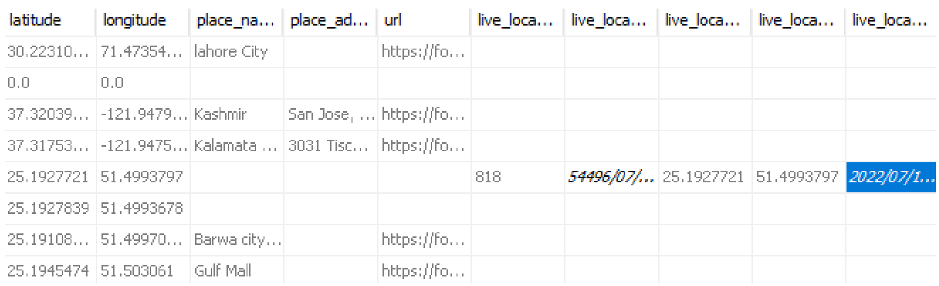
-5767174191651600043_120

-5767174191651600044_109

-5767174191651600044_120

-5767174191651600046_121

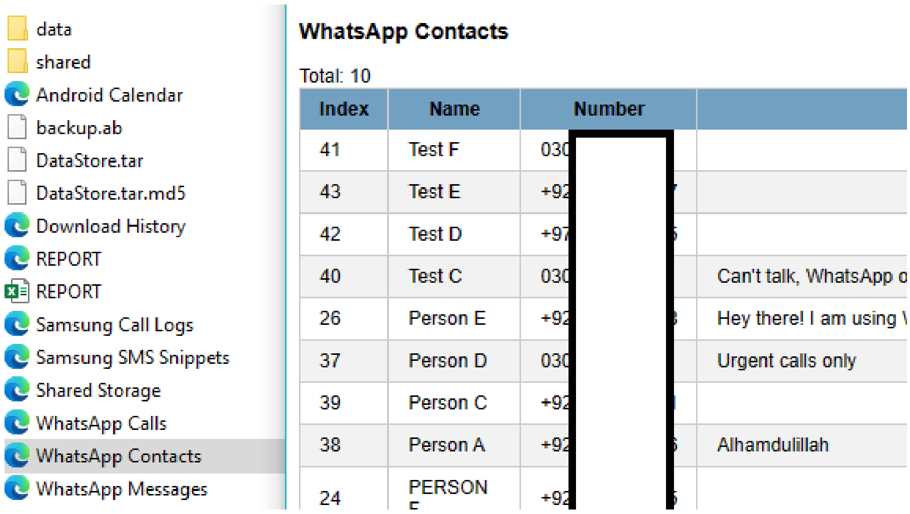
Table 5.75– Andriller Test Result MDT-64, MDT-65, MDT-99, MDT-100, MDT-109, MDT-110

Test case id	MDT-120
Test case result	Successful in combination with Autopsy database viewer.
Test case analysis	Andriller was able to extract geolocation data present in WhatsApp chat messages.
Screenshots	

latitude	longitude	place_na…	place_ad…	url	live_loca…	live_loca…	live_loca…	live_loca…	live_loca…
30.22310…	71.47354…	lahore City		https://fo…					
0.0	0.0								
37.32039…	-121.9479…	Kashmir	San Jose, …	https://fo…					
37.31753…	-121.9475…	Kalamata …	3031 Tisc…	https://fo…					
25.1927721	51.4993797				818	54496/07/…	25.1927721	51.4993797	2022/07/1…
25.1927839	51.4993678								
25.19108…	51.49970…	Barwa city…		https://fo…					
25.1945474	51.503061	Gulf Mall		https://fo…					

Table 5.76– Andriller Test Result MDT-120

Test case id	MDT-121

Test case result	As expected.
Test case analysis	Andriller successfully presented the text with the correct character glyphs.
Screenshots	

- data
- shared
- Android Calendar
- backup.ab
- DataStore.tar
- DataStore.tar.md5
- Download History
- REPORT
- REPORT
- Samsung Call Logs
- Samsung SMS Snippets
- Shared Storage
- WhatsApp Calls
- WhatsApp Contacts
- WhatsApp Messages

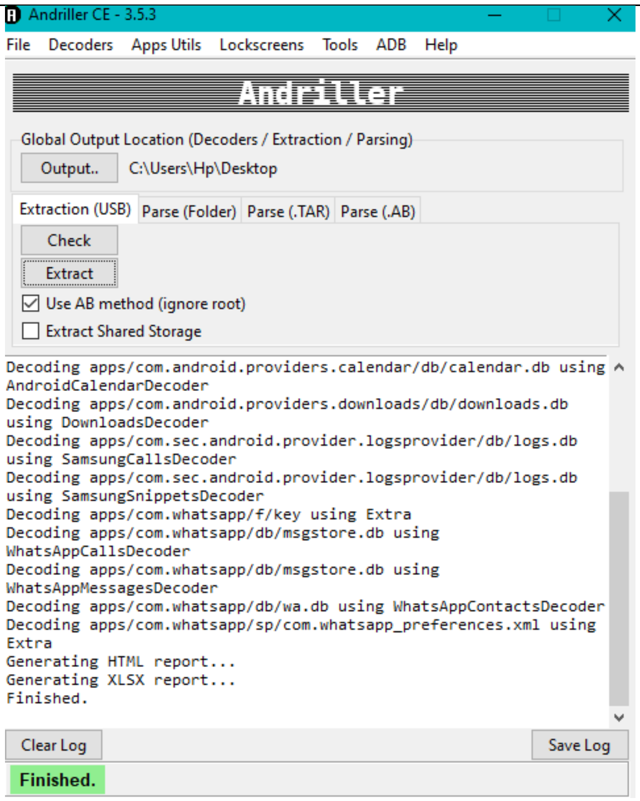
WhatsApp Contacts

Total: 10

Index	Name	Number	
41	Test F	[redacted]	
43	Test E	[redacted]	
42	Test D	[redacted]	
40	Test C	[redacted]	Can't talk, WhatsApp o
26	Person E	[redacted]	Hey there! I am using
37	Person D	[redacted]	Urgent calls only
39	Person C	[redacted]	
38	Person A	[redacted]	Alhamdulillah
24	PERSON E	[redacted]	

Table 5.77– Andriller Test Result MDT-121

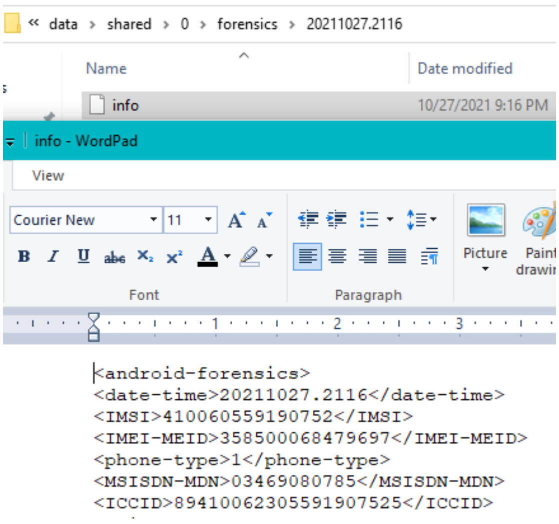
Test case id	MDT-127
Test case result	As expected.
Test case analysis	Andriller successfully created an image file of the device file system.
Screenshots	

```
Decoding apps/com.android.providers.calendar/db/calendar.db using
AndroidCalendarDecoder
Decoding apps/com.android.providers.downloads/db/downloads.db
using DownloadsDecoder
Decoding apps/com.sec.android.provider.logsprovider/db/logs.db
using SamsungCallsDecoder
Decoding apps/com.sec.android.provider.logsprovider/db/logs.db
using SamsungSnippetsDecoder
Decoding apps/com.whatsapp/f/key using Extra
Decoding apps/com.whatsapp/db/msgstore.db using
WhatsAppCallsDecoder
Decoding apps/com.whatsapp/db/msgstore.db using
WhatsAppMessagesDecoder
Decoding apps/com.whatsapp/db/wa.db using WhatsAppContactsDecoder
Decoding apps/com.whatsapp/sp/com.whatsapp_preferences.xml using
Extra
Generating HTML report...
Generating XLSX report...
Finished.
```

Table 5.78– Andriller Test Result MDT-127

Test case id	MDT-132, MDT-133, MDT-134
Test case result	As expected.
Test case analysis	Andriller successfully presented the ICCID, IMSI, and MSISDN from the image file.
Screenshots	

« data › shared › 0 › forensics › 20211027.2116

Name	Date modified
info	10/27/2021 9:16 PM

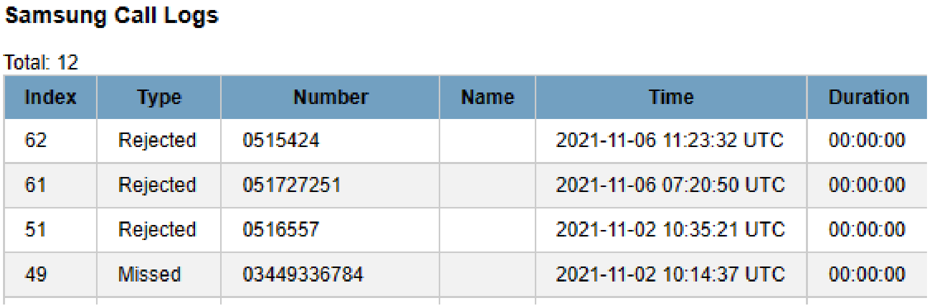
info - WordPad

```
<android-forensics>
<date-time>20211027.2116</date-time>
<IMSI>410060559190752</IMSI>
<IMEI-MEID>358500068479697</IMEI-MEID>
<phone-type>1</phone-type>
<MSISDN-MDN>03469080785</MSISDN-MDN>
<ICCID>89410062305591907525</ICCID>
```

Table 5.79– Andriller Test Result MDT-132, MDT-133, MDT-134

Test case id	MDT-135
Test case result	Not checked.
Test case analysis	Andriller was unable to detect the ADNs from an image file.
Screenshots	-

Table5.80 –Andriller Test Result MDT-135

Test case id	MDT-136
Test case result	As expected.
Test case analysis	Andriller successfully displayed the LND from an image file.
Screenshots	

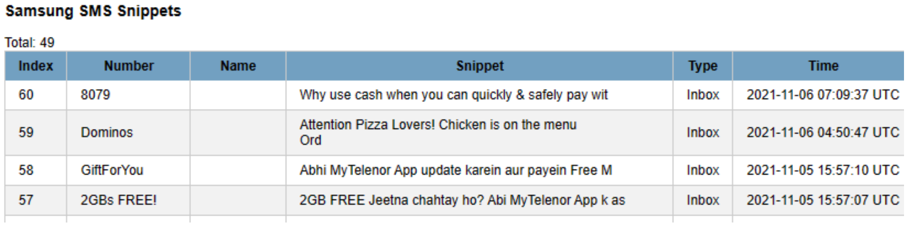
Samsung Call Logs

Total: 12

Index	Type	Number	Name	Time	Duration
62	Rejected	0515424		2021-11-06 11:23:32 UTC	00:00:00
61	Rejected	051727251		2021-11-06 07:20:50 UTC	00:00:00
51	Rejected	0516557		2021-11-02 10:35:21 UTC	00:00:00
49	Missed	03449336784		2021-11-02 10:14:37 UTC	00:00:00

Table 5.81– Andriller Test Result MDT-136

Test case id	MDT-137
Test case result	As expected.

Test case analysis	Andriller successfully displayed SMS messages from the image file.
Screenshots	 **Samsung SMS Snippets** Total: 49 <table placeholder below>

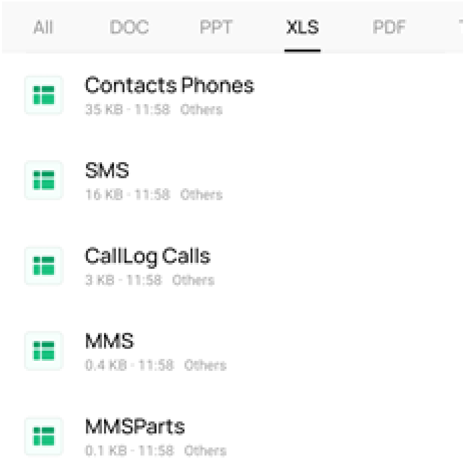
Samsung SMS Snippets

Total: 49

Index	Number	Name	Snippet	Type	Time
60	8079		Why use cash when you can quickly & safely pay wit	Inbox	2021-11-06 07:09:37 UTC
59	Dominos		Attention Pizza Lovers! Chicken is on the menu Ord	Inbox	2021-11-06 04:50:47 UTC
58	GiftForYou		Abhi MyTelenor App update karein aur payein Free M	Inbox	2021-11-05 15:57:10 UTC
57	2GBs FREE!		2GB FREE Jeetna chahtay ho? Abi MyTelenor App k as	Inbox	2021-11-05 15:57:07 UTC

Table 5.82– Andriller Test Result MDT-137

5.3.3 AFLogical Test Results Report



Contacts Phones
35 KB · 11:58 Others

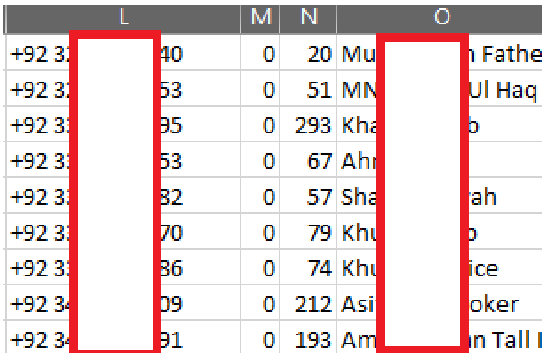
SMS
16 KB · 11:58 Others

CallLog Calls
3 KB · 11:58 Others

MMS
0.4 KB · 11:58 Others

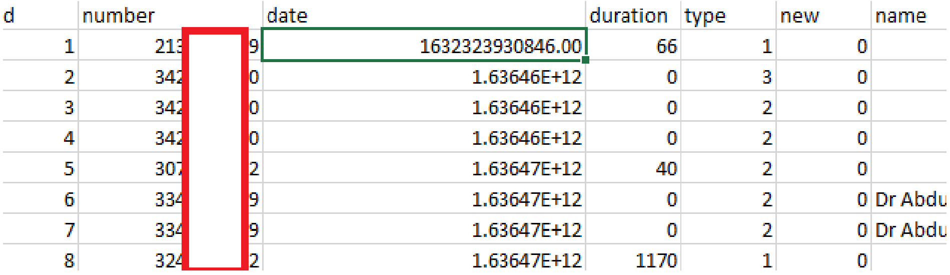
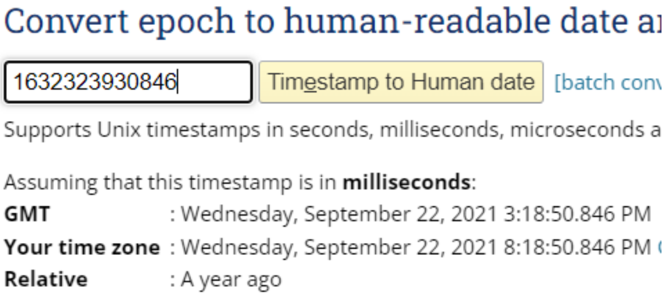
MMSParts
0.1 KB · 11:58 Others

Fig 5.4--AFLogical overall extraction results

Test case id	MDT-03
Test case result	As expected
Test case analysis	AFLogical successfully extracted the address book data.
Screenshots	

L	M	N	O
+92 3[redacted]40	0	20	Mu[redacted]n Fathe
+92 3[redacted]53	0	51	MN[redacted]Ul Haq
+92 3[redacted]95	0	293	Kha[redacted]b
+92 3[redacted]53	0	67	Ahr[redacted]
+92 3[redacted]82	0	57	Sha[redacted]ah
+92 3[redacted]70	0	79	Khu[redacted]b
+92 3[redacted]86	0	74	Khu[redacted]ice
+92 34[redacted]09	0	212	Asi[redacted]oker
+92 34[redacted]91	0	193	Am[redacted]n Tall I

Table 5.83– AFLogical Test Result MDT-03

Test case id	MDT-05, MDT-06, MDT-07, MDT-08, MDT-09
Test case result	As expected.
Test case analysis	AFLogical successfully extracted the call log data. The date timestamp was converted to a human readable format using an epoch converter online.
Screenshots	 

d	number	date	duration	type	new	name
1	213[redacted]9	1632323930846.00	66	1	0	
2	342[redacted]0	1.63646E+12	0	3	0	
3	342[redacted]0	1.63646E+12	0	2	0	
4	342[redacted]0	1.63646E+12	0	2	0	
5	307[redacted]2	1.63647E+12	40	2	0	
6	334[redacted]9	1.63647E+12	0	2	0	Dr Abdu
7	334[redacted]9	1.63647E+12	0	2	0	Dr Abdu
8	324[redacted]2	1.63647E+12	1170	1	0	

Convert epoch to human-readable date a

1632323930846

Supports Unix timestamps in seconds, milliseconds, microseconds a

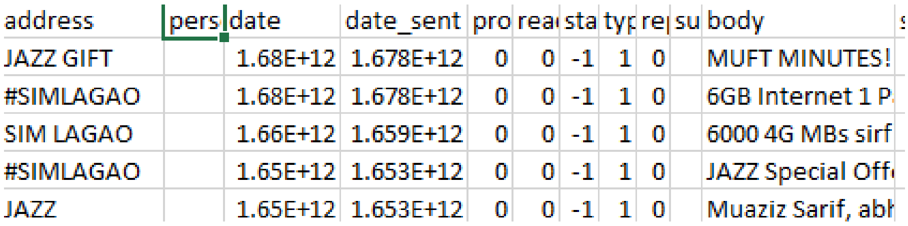
Assuming that this timestamp is in **milliseconds**:

GMT : Wednesday, September 22, 2021 3:18:50.846 PM

Your time zone : Wednesday, September 22, 2021 8:18:50.846 PM

Relative : A year ago

Table 5.84– AFLogical Test Result MDT-05, MDT-06, MDT-07, MDT-08, MDT-09

Test case id	MDT-10, MDT-13
Test case result	As expected.
Test case analysis	AFLogical successfully extracted the local messages with time stamps.
Screenshots	

address	pers	date	date_sent	pro	rea	sta	typ	re	su	body	s
JAZZ GIFT		1.68E+12	1.678E+12	0	0	-1	1	0		MUFT MINUTES!	
#SIMLAGAO		1.68E+12	1.678E+12	0	0	-1	1	0		6GB Internet 1 P	
SIM LAGAO		1.66E+12	1.659E+12	0	0	-1	1	0		6000 4G MBs sirf	
#SIMLAGAO		1.65E+12	1.653E+12	0	0	-1	1	0		JAZZ Special Offe	
JAZZ		1.65E+12	1.653E+12	0	0	-1	1	0		Muaziz Sarif, abh	

Table 5.85–AFLogical Test Result MDT-10, MDT-13

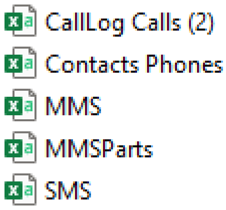
Test case id	MDT-01,MDT-02 … MDT-04, MDT-11, MDT-12, MDT-14, MDT-15, …. MDT-140
Test case result	Not checked.
Test case analysis	AFLogical was unable to extract any application-based data.
Screenshots	 CallLog Calls (2) Contacts Phones MMS MMSParts SMS

Table 5.86–AFLogical Test Result MDT-01,MDT-02 … MDT-04, MDT-11, MDT-12, MDT-14, MDT-15, …. MDT-140

5.4 Comparative Analysis of the Forensic Tools

Tables 5.87(a), 5.87(b), and 5.87(c) provide the core and optional test results of the three tools respectively. The test result is stated as either 0,1 or 2 where 0 represents the inability of the tool to perform the given test case successfully, 1 represents compliance with the test case and 2 represents that the test case is successful when the targeted tool is used in combination with another tool. This table provides a comparative view of the results obtained from the framework and directly maps the tools onto the framework.

Profile	TestCase ID	Autopsy	Andriller	AFLogical
Image file artifacts	MDT-01	1	0	0
	MDT-02	1	1	0
	MDT-03	1	2	1
	MDT-04	1	2	0
	MDT-05	1	1	1
	MDT-06	1	1	1
	MDT-07	1	1	1
	MDT-08	1	1	1
	MDT-09	1	1	1
	MDT-10	1	1	1
	MDT-11	N/A	N/A	N/A
	MDT-12	1	2	0
	MDT-13	1	1	1
	MDT-14	N/A	N/A	N/A
	MDT-15	1	2	0

	MDT-16	1	1	0
	MDT-17	1	1	0
	MDT-18	1	1	0
	MDT-19	1	2	0
	MDT-20	1	1	0
	MDT-21	1	0	0
	MDT-22	1	0	0
	MDT-23	1	0	0
	MDT-24	1	0	0
	MDT-25	1	0	0

Table 5.87(a)– Comparative Test Results of Evaluation of Tools

Profile	**TestCase ID**	**Autopsy**			**Andriller**			**AFLogical**		
		Whatsapp	**Telegram**	**Kalamtime**	**Whatsapp**	**Telegram**	**Kalamtime**	**Whatsapp**	**Telegram**	**Kalamtime**
Image file artifacts	MDT-26	1	1	1	1	0	0	0	0	0
	MDT-27	1	1	1	2	0	0	0	0	0
	MDT-28	1	1	1	1	0	0	0	0	0
	MDT-29	0	0	0	0	0	0	0	0	0
	MDT-30	1	0	0	0	0	0	0	0	0
	MDT-31	1	0	1	1	0	0	0	0	0
	MDT-32	1	0	1	1	0	0	0	0	0
	MDT-33	1	1	1	1	0	0	0	0	0
	MDT-34	1	2	1	1	0	0	0	0	0
	MDT-35	1	0	1	1	0	0	0	0	0
	MDT-36	1	0	1	1	0	0	0	0	0
	MDT-37	1	1	1	2	0	0	0	0	0
	MDT-38	1	1	1	2	0	0	0	0	0
	MDT-39	0	0	0	0	0	0	0	0	0
	MDT-40	1	0	N/A	1	0	N/A	0	0	N/A
	MDT-41	1	0	N/A	1	0	N/A	0	0	N/A
	MDT-42	1	0	N/A	2	0	N/A	0	0	N/A
	MDT-43	1	0	N/A	2	0	N/A	0	0	N/A
	MDT-44	1	0	N/A	1	0	N/A	0	0	N/A
	MDT-45	1	0	N/A	1	0	N/A	0	0	N/A
	MDT-46	1	1	N/A	2	0	N/A	0	0	N/A
	MDT-47	1	1	N/A	2	0	N/A	0	0	N/A
	MDT-48	0	0	N/A	0	0	N/A	0	0	N/A
	MDT-49	0	0	N/A	0	0	N/A	0	0	N/A
	MDT-50	1	0	1	1	0	0	0	0	0
	MDT-51	1	0	1	1	0	0	0	0	0
	MDT-52	1	1	1	1	0	0	0	0	0
	MDT-53	1	1	1	1	0	0	0	0	0
	MDT-54	0	0	1	0	0	0	0	0	0
	MDT-55	0	0	1	0	0	0	0	0	0
	MDT-56	1	2	0	2	0	0	0	0	0
	MDT-57	1	0	1	2	0	0	0	0	0
	MDT-58	0	0	1	0	0	0	0	0	0
	MDT-59	0	0	1	0	0	0	0	0	0
	MDT-60	1	2	1	2	0	0	0	0	0
	MDT-61	1	0	0	2	0	0	0	0	0
	MDT-62	1	0	1	1	0	0	0	0	0

	MDT-63	1	0	1	1	0	0	0	0	0
	MDT-64	1	1	1	1	1	1	0	0	0
	MDT-65	1	1	1	1	1	1	0	0	0
	MDT-66	0	N/A	1	0	N/A	N/A	0	N/A	N/A
	MDT-67	1	N/A	1	2	N/A	N/A	0	N/A	N/A
	MDT-68	0	N/A	1	0	N/A	N/A	0	N/A	N/A
	MDT-69	0	N/A	1	0	N/A	N/A	0	N/A	N/A
	MDT-70	0	N/A	0	0	N/A	N/A	0	N/A	N/A
	MDT-71	0	N/A	0	0	N/A	N/A	0	N/A	N/A
	MDT-72	0	N/A	0	0	N/A	N/A	0	N/A	N/A
	MDT-73	0	N/A	0	0	N/A	N/A	0	N/A	N/A
	MDT-74	0	N/A	0	0	N/A	N/A	0	N/A	N/A
	MDT-75	1	2	1	2	0	0	0	0	0
	MDT-76	1	0	1	2	0	0	0	0	0
	MDT-77	0	0	0	0	0	0	0	0	0
	MDT-78	1	0	1	0	0	0	0	0	0
	MDT-79	1	2	1	1	0	0	0	0	0
	MDT-80	1	2	1	1	0	0	0	0	0
	MDT-81	1	0	N/A	1	0	N/A	0	0	N/A
	MDT-82	1	1	N/A	1	0	N/A	0	0	N/A
	MDT-83	1	1	N/A	1	0	N/A	0	0	N/A
	MDT-84	1	0	N/A	0	0	N/A	0	0	N/A
	MDT-85	0	0	N/A	0	0	N/A	0	0	N/A
	MDT-86	1	0	1	0	0	0	0	0	0
	MDT-87	1	1	1	1	0	0	0	0	0
	MDT-88	1	1	1	0	0	0	0	0	0
	MDT-89	0	0	1	0	0	0	0	0	0
	MDT-90	0	0	0	0	0	0	0	0	0
	MDT-91	1	1	1	2	0	0	0	0	0
	MDT-92	1	0	1	2	0	0	0	0	0
	MDT-93	0	0	1	0	0	0	0	0	0
	MDT-94	0	0	0	0	0	0	0	0	0
	MDT-95	1	2	1	2	0	0	0	0	0
	MDT-96	1	0	1	2	0	0	0	0	0
	MDT-97	1	0	1	1	0	0	0	0	0
	MDT-98	1	1	1	1	0	0	0	0	0
	MDT-99	1	1	1	1	1	1	0	0	0
	MDT-100	1	1	1	1	1	1	0	0	0
	MDT-101	1	0	N/A	2	0	N/A	0	0	N/A
	MDT-102	1	0	N/A	0	0	N/A	0	0	N/A
	MDT-103	1	0	N/A	0	0	N/A	0	0	N/A
	MDT-104	1	1	N/A	1	0	N/A	0	0	N/A
	MDT-105	1	2	N/A	1	0	N/A	0	0	N/A
	MDT-106	1	1	N/A	2	0	N/A	0	0	N/A
	MDT-107	1	1	N/A	0	0	N/A	0	0	N/A
	MDT-108	1	1	N/A	1	0	N/A	0	0	N/A
	MDT-109	1	1	N/A	1	1	N/A	0	0	N/A
	MDT-110	1	1	N/A	1	1	N/A	0	0	N/A
	MDT-111	N/A	0	1	N/A	0	0	N/A	0	0
	MDT-112	N/A	0	0	N/A	0	0	N/A	0	0
	MDT-113	N/A	1	1	N/A	0	0	N/A	0	0
	MDT-114	N/A	2	1	N/A	0	0	N/A	0	0
	MDT-115	N/A	0	1	N/A	0	0	N/A	0	0

	MDT-116	N/A	0	1	N/A	0	0	N/A	0	0
	MDT-117	N/A	1	0	N/A	0	0	N/A	0	0
	MDT-118	N/A	1	1	N/A	0	0	N/A	0	0
	MDT-119	N/A	0	0	N/A	0	0	N/A	0	0

Table 5.87(b)– Comparative Test Results of Evaluation of Tools w.r.t social media applications

Profile	TestCase ID	Autopsy	Andriller	Aflogical
Image file artifacts	MDT-120	1	2	0
	MDT-121	1	1	0
	MDT-122	N/A	0	0
	MDT-123	N/A	0	0
Image file acquisition	MDT-124	N/A	0	0
	MDT-125	N/A	0	0
	MDT-126	N/A	0	0
	MDT-127	N/A	1	0
	MDT-128	N/A	0	0
	MDT-129	N/A	0	0
UICC acquisition	MDT-130	N/A	0	0
	MDT-131	0	0	0
	MDT-132	1	1	0
	MDT-133	1	1	0
	MDT-134	1	1	0
	MDT-135	0	0	0
	MDT-136	1	1	0
	MDT-137	1	1	0
	MDT-138	0	0	0
	MDT-139	0	0	0
Deleted data artifacts	MDT-140	0	0	0
SQLite database	MDT-141	1	N/A	N/A
	MDT-142	1	N/A	N/A
	MDT-143	0	N/A	N/A
	MDT-144	0	N/A	N/A
	MDT-145	0	N/A	N/A
	MDT-146	0	N/A	N/A
	MDT-147	0	N/A	N/A
	MDT-148	0	N/A	N/A
	MDT-149	0	N/A	N/A
	MDT-150	0	N/A	N/A
	MDT-151	0	N/A	N/A

Table 5.87(c)– Comparative Test Results of Evaluation of Tools

The test results of the tools indicate that Autopsy confirms most of the core test cases, whereas AFLogical confirms the least. In the case of social media applications, Autopsy confirmed most of the test cases. Andriller specifically extracted WhatsApp artifacts separately and presented them in XML format, but it did not extract much data from other social media applications, other than media files. AFLogical only extracted logical mobile data, and was unable to extract any application-related data.

5.5 Discussion

Autopsy was able to confirm 56% of the mobile device test cases (excluding social media application test cases), however, 19% of them involved features that were non-existent in the test device and autopsy. The MMS feature did not work in the test device and autopsy, the image acquisition feature did not exist. But autopsy accepts all kinds of images whether it’s logical, physical, or selected files only. 67% of social media application test cases were successfully passed by autopsy in the case of WhatsApp, however, 10% of them involved features that did not exist in WhatsApp, i.e. secret message and message editing. In the case of Telegram, 31% of social media application test cases were passed by autopsy, and 10% of the test cases were passed by autopsy in combination with the SQLite DB Browser tool, as it was unable to represent data stored in BLOB format. 10% of the test cases consisted of features that did not exist in the Telegram app, namely the status uploading feature. 56% of the test cases were passed by Autopsy in the case of the KalamTime application, however, 27 % of them consisted of features that did not exist in KalamTime. These features included starred messages, disappearing messages, and broadcasts.

Andriller confirmed 33% of the mobile device test cases (excluding social media application test cases), and 9% of the test cases succeeded in combination with Autopsy because Andriller does not consist of its own database browser. 23% of the time the features being tested did not exist in the test device and Andriller. These features were MMS features in the case of the test device, and SQLite database browsing features in the case of Andriller. Andriller confirmed 38% of the social media application test cases in the case of WhatsApp, and 21% of them Andriller passed in combination with using the Autopsy database viewing feature. 10% of the test cases involved features that do not exist in WhatsApp. As Andriller was unable to extract the Telegram database, it only presented media files sent or received. That comprised 6% of the social media application test cases, and 10% of them involved features non-existent in Telegram. Similarly, 4% of test cases succeeded in the case of the KalamTime application, 27% of them consisting of features that did not exist in KalamTime.

AFLogical confirmed 14% of the mobile device test cases (excluding social media application test cases), 19% of the time the features being tested did not exist in the test device and AFLogical. AFLogical was unable to extract any social media application data from the test device. It did not confirm any of the social media application-related test cases.

5.6 Summary

This chapter presents detailed test results of the experiments. A list of features of the forensic tools is presented in the beginning. After this, the working environment, specification of forensic tools, and experimental analysis are presented. Results are presented and discussed at the end of this chapter.

6. Conclusion and Future Work

This Chapter concludes the presented thesis and highlights potential future research directions. It describes different research prospects of our research and identifies open research problems that still need to be solved by the research community.

Substantial research has been carried out in the mobile forensics discipline in recent years and the scope for discovery, design, and improvements in the techniques and tools involved is vast. The challenges involved in investigating and testing all the features with the tool become time-consuming and it may need to be automated. However, a product (specifically a software tool) needs to be quality tested before being introduced to mainstream users. A convenient aspect of the evaluation frameworks can be revisited and improved indefinitely, as the tools evolve and advance. More test assertions can be added with additional test cases. The continuous technical hit and trial is an attempt to set standards for the tools to achieve. These standards complement all areas of life in which the tool may be employed, e.g., criminal investigation, commercial use, or academic research and study.

6.1 Conclusion

This research work compares three open-source mobile forensic tools, namely Autopsy, Andriller, and AFLogical, based on their ability to extract data from social media applications, namely WhatsApp, Telegram, and KalamTime. The evaluation of these tools follows the conformance methodology provided by NIST, called CFTT. Additional test cases were added against the test assertions provided by CFTT, to evaluate the forensic tools, mainly to test the social media application data. Most of the test cases were derived from the core test assertions that came under the “Image file artifacts” profile, i.e., 123 test cases. The rest of the test cases were derived from optional assertions. From the “Image file acquisition” profile, 6 test cases were derived. From the “UICC acquisition” profile, 10 test cases were derived. One test case was derived from the “deleted data artifacts” profile and 11 test cases were derived from the “SQLite database” profile.

The comparative analysis of the results showed that Autopsy performed the most as compared to the other two forensic tools, it extracted all the databases related to the applications (from the physical image file provided to it) and presented the data in its database viewer, and in the case of WhatsApp, it showed the results separately as well, such as calls and messages, that the analyst can navigate to, directly. However, the database viewer in Autopsy was unable to present BLOB data. Andriller extracted data from the mobile device directly but presented mostly WhatsApp data in the form of an XML document. It showed media files of other apps and was unable to extract their databases. Andriller did not have its database viewer. AFLogical was unsuccessful in recovering any application data, but only local data such as calls and SMS data, presented in the form of an XML document.

It is evident that every tool has some shortcomings, but the results obtained from the forensic tool evaluation highlight all the areas that can be improved. These shortcomings can be used to improve the existing tools. For example, Autopsy shall have image extraction capabilities and Andriller should have its database viewer. AFLogical can be expanded to extract application data.

6.2 Future Work

This research work was limited to three Android applications, namely WhatsApp, Telegram, and KalamTime. Further, forensic tools were also limited to open-source tools. In the future, more popular social media applications can be tested and other forensic tools can be used to forensically analyze. Meanwhile, newer updates of applications and forensic tools can be tested for the latest results.

Bibliography

[1] Federal Investigation Agency. (2022). Fia.gov.pk. https://www.fia.gov.pk/ccw

[2] Laricchia, F. (2019, June 29). Mobile OS market share 2019 | Statista. Statista; Statista. https://www.statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009/

[3] Global Social Media Statistics — DataReportal – Global Digital Insights. (n.d.). DataReportal – Global Digital Insights. https://datareportal.com/social-media-users#:~:text=Detailed%20analysis%20by%20the%20team,of%20the%20total%20global%20population.

[4] AskJamieTurner. (2020, July 27). 5 Industries that Benefit the Most from Social Media. 60 Second Marketer @AskJamieTurner. https://60secondmarketer.com/2020/07/27/5-industries-that-benefit-the-most-from-social-media/

[5] Swenson. (2006, September 14). NIST Guide Details Forensic Practices for Data Analysis. NIST. https://www.nist.gov/news-events/news/2006/09/nist-guide-details-forensic-practices-data-analysis

[6] Packtpub.com. https://subscription.packtpub.com/book/networking-and-servers/9781788625005/1/ch01lvl1sec12/commercial-tools-available-in-the-field-of-digital-forensics

[7] Vanessa. (2018). The Best Open Source Digital Forensic Tools. H-11 Digital Forensics. https://h11dfs.com/the-best-open-source-digital-forensic-tools/

[8] OpenText. (2021). EnCase Forensic Software - Top Digital Forensics and Investigations Solution. Security.opentext.com. https://security.opentext.com/encase-forensic

[9] Mobile Forensics - Definition, Uses, and Principles. (2022, March 1). GeeksforGeeks. https://www.geeksforgeeks.org/mobile-forensics-definition-uses-and-principles/

[10] Sathe, S. C., & Dongre, N. M. (2018). Data acquisition techniques in mobile forensics. 2018 2nd International Conference on Inventive Systems and Control (ICISC). https://doi.org/10.1109/icisc.2018.8399079

[11] Pinchas. (2019, December 3). Cases Where WhatsApp Chats Was Used as Evidence in Court. TeleMessage. https://www.telemessage.com/whatsapp-ediscovery-cases-

where-whatsapp-chats-was-used-as-evidence-in-court/

[12] Crime and social media | Special Report | thenews.com.pk. (n.d.). Www.thenews.com.pk. https://www.thenews.com.pk/tns/detail/917575-crime-and-social-media

[13] Five Common Types of Social Media Crime. (2017, February 22). FindLaw. https://www.findlaw.com/legalblogs/criminal-defense/5-common-types-of-social-media-crime/

[14] Anglano, C., Canonico, M., & Guazzone, M. (2020). The Android Forensics Automator (AnForA): A tool for the Automated Forensic Analysis of Android Applications. Computers & Security, 88, 101650. https://doi.org/10.1016/j.cose.2019.101650

[15] Lin, X., Chen, T., Zhu, T., Yang, K., & Wei, F. (2018). Automated forensic analysis of mobile applications on Android devices. Digital Investigation, 26, S59–S66. https://doi.org/10.1016/j.diin.2018.04.012

[16] Lwin, H. H., Aung, W. P., & Lin, K. K. (2020, February 1). Comparative Analysis of Android Mobile Forensics Tools. IEEE Xplore. https://doi.org/10.1109/ICCA49400.2020.9022838

[17] Alissa, K., Almubairik, N. A., Alsaleem, L., Alotaibi, D., Aldakheel, M., Alqhtani, S., Saqib, N., Brahimi, S., & Alshahrani, M. (2019). A comparative study of WhatsApp forensics tools. SN Applied Sciences, 1(11). https://doi.org/10.1007/s42452-019-1312-8

[18] Nurhairani, H., & Riadi, I. (2019). Analysis Mobile Forensics on Twitter Application using the National Institute of Justice (NIJ) Method. International Journal of Computer Applications, 177(27), 35–42. https://www.ijcaonline.org/archives/volume177/number27/31077-2019919749

[19] Pribadi, B., Rosdiana, S., & Arifin, S. (2023). Digital forensics on facebook messenger application in an android smartphone based on NIST SP 800-101 R1 to reveal digital crime cases. Procedia Computer Science, 216, 161–167. https://doi.org/10.1016/j.procs.2022.12.123

[20] Bhat, W. A., Jalal, M., Khan, S. A., Shah, F. F., & Wani, M. A. (2019). Forensic analysis of Sync.com and FlipDrive cloud applications on Android platform. Forensic Science International, 302, 109845. https://doi.org/10.1016/j.forsciint.2019.06.003

[21] Instagram Forensic Analysis Revisited: Does anything really vanish? (2021b,

October 31). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9615910

[22] Mahr, A., Cichon, M., Mateo, S., Grajeda, C., & Baggili, I. (2021). Zooming into the pandemic! A forensic analysis of the Zoom Application. Forensic Science International: Digital Investigation, 36, 301107. https://doi.org/10.1016/j.fsidi.2021.301107

[23] Forensic analysis of TikTok application to seek digital artifacts on Android smartphone. (2020, October 1). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/9140739

[24] Menahil, A., Iqbal, W., Iftikhar, M., Shahid, W. B., Mansoor, K., & Rubab, S. (2021). Forensic Analysis of Social Networking Applications on an Android Smartphone. Wireless Communications and Mobile Computing, 2021, 1–36. https://doi.org/10.1155/2021/5567592

[25] Kim, G., Kim, S., Park, M., Park, Y., Lee, I., & Kim, J. (2021). Forensic analysis of instant messaging apps: Decrypting Wickr and private text messaging data. Forensic Science International: Digital Investigation, 37, 301138. https://doi.org/10.1016/j.fsidi.2021.301138

[26] Bashir, S., Abbas, H., Shafqat, N., Iqbal, W., & Saleem, K. (2019). Forensic Analysis of LinkedIn's Desktop Application on Windows 10 OS. In Advances in intelligent systems and computing. Springer Nature. https://doi.org/10.1007/978-3-030-14070-0_9

[27] Iqbal, F., Motylinski, M., & MacDermott, A. (2021). Discord Server Forensics: Analysis and Extraction of Digital Evidence. In New Technologies, Mobility and Security. https://doi.org/10.1109/ntms49979.2021.9432654

[28] Barros, A. S., Almeida, R. S. R., Melo, T., & Frade, M. (2022). Forensic Analysis of the Bumble Dating App for Android. Forensic Sciences, 2(1), 201–221. https://doi.org/10.3390/forensicsci2010016

[29] A Digital Forensics Analysis for Detection of The Modified COVID-19 Mobile Application. (2020, September 1). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/9219416

[30] Digital Forensic Analysis Of Michat Application On Android As Digital Proof In Handling Online Prostitution Cases | JELIKU (Jurnal Elektronik Ilmu Komputer Udayana). (n.d.). https://ojs.unud.ac.id/index.php/JLK/article/view/64489

[31] Ichsan, A. N., & Riadi, I. (2021). Mobile Forensic on Android-based IMO

Messenger Services using Digital Forensic Research Workshop (DFRWS) Method. International Journal of Computer Applications, 174(18), 34–40. https://doi.org/10.5120/ijca2021921076

[32] Prayogo, A. G., & Riadi, I. (2022). Digital Forensic Signal Instant Messages Services in Case of Cyberbullying using Digital Forensic Research Workshop Method. International Journal of Computer Applications, 184(32), 21–29. https://doi.org/10.5120/ijca2022922393

[33] Gandhi, T. M. (2021). Forensic Analysis of GroupMe on Android and iOS Smartphones. Figshare. https://doi.org/10.25394/PGS.15079083.v1

[34] O. K. Appiah-Kubi, "Evaluation of UFED Physical Pro 1.1.3.8 and XRY 5.0 : Tools for Extracting e-Evidence from Mobile Devices," Thesis, 2011.

[35] K. Piirainen, R. Gonzalez, and G. Kolfschoten, "Quo Vadis, Design Science? A Survey of Literature', in Global Perspectives on Design Science Research, International Conference on design science research in information systems, pp. 93–108," 2010.

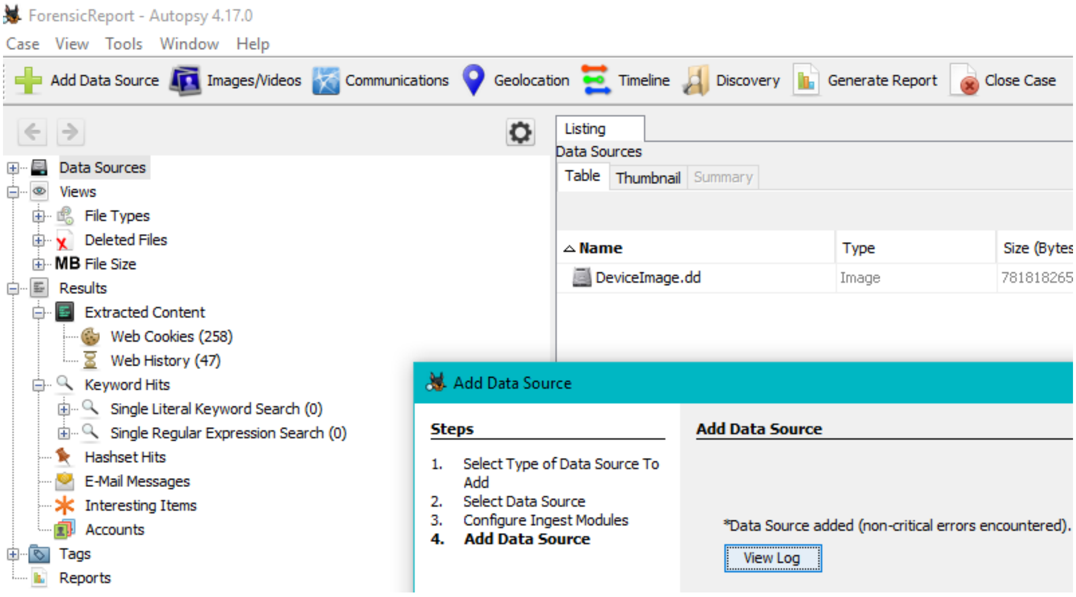
[36] jbass, "Overview of Conformance Testing", NIST, 8 Sept. 2010, https://www.nist.gov/itl/ssd/information-systems-group/overview-conformance-testing.

[37] E. H. Holder and L. O. Robinson, "Special Report Test Results for Digital Data Acquisition Tool", CFTT, NIST, Nij, 2008.

[38] Quora. (2019, June 4). How Are Criminals Using Smart Devices To Commit Crimes? Forbes. https://www.forbes.com/sites/quora/2019/06/04/how-are-criminals-using-smart-devices-to-commit-crimes/

[39] Khalid, Z., Iqbal, F., Kamoun, F., Hussain, M., & Khan, L. A. (2021, October). Forensic analysis of the Cisco WebEx application. In *2021 5th Cyber Security in Networking Conference (CSNet)* (pp. 90-97). IEEE.

APPENDIX A – AUTOPSY REPORT



- Data Sources
- Views
  - File Types
  - Deleted Files
  - MB File Size
- Results
  - Extracted Content
    - Web Cookies (258)
    - Web History (47)
  - Keyword Hits
    - Single Literal Keyword Search (0)
    - Single Regular Expression Search (0)
  - Hashset Hits
  - E-Mail Messages
  - Interesting Items
  - Accounts
- Tags
- Reports

Data Sources

Name	Type	Size (Bytes
DeviceImage.dd	Image	781818265

Add Data Source

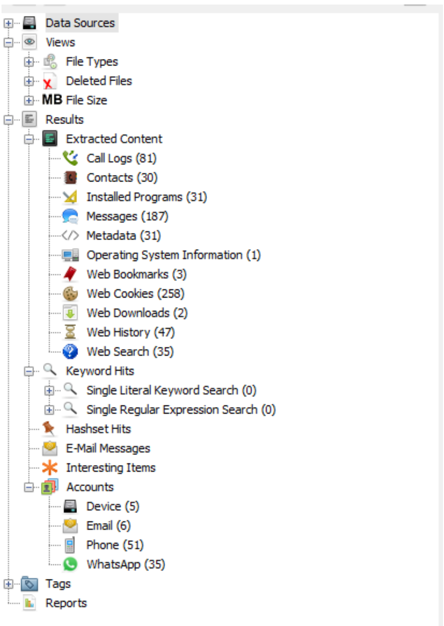
Steps

1. Select Type of Data Source To Add
2. Select Data Source
3. Configure Ingest Modules
4. **Add Data Source**

Add Data Source

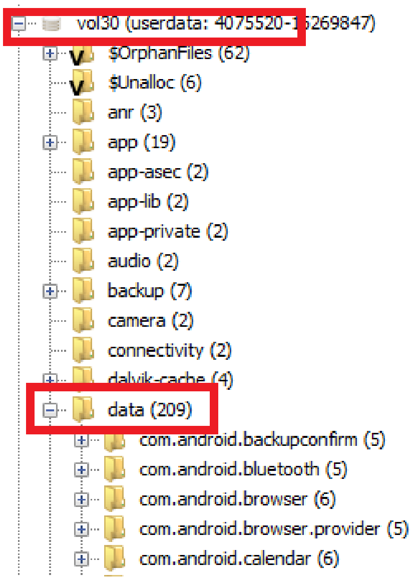
*Data Source added (non-critical errors encountered).

Fig A.1 – Autopsy physical image analysis



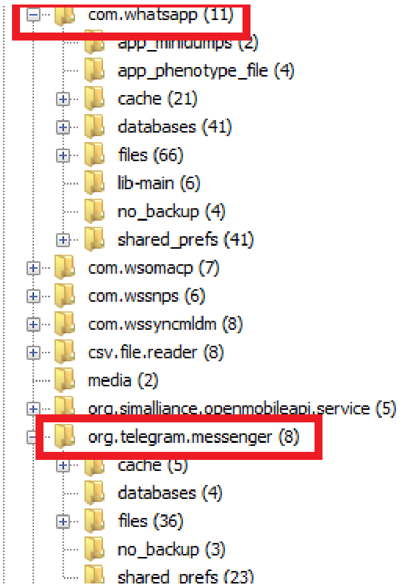
- Data Sources
- Views
  - File Types
  - Deleted Files
  - MB File Size
- Results
  - Extracted Content
    - Call Logs (81)
    - Contacts (30)
    - Installed Programs (31)
    - Messages (187)
    - Metadata (31)
    - Operating System Information (1)
    - Web Bookmarks (3)
    - Web Cookies (258)
    - Web Downloads (2)
    - Web History (47)
    - Web Search (35)
  - Keyword Hits
    - Single Literal Keyword Search (0)
    - Single Regular Expression Search (0)
  - Hashset Hits
  - E-Mail Messages
  - Interesting Items
  - Accounts
    - Device (5)
    - Email (6)
    - Phone (51)
    - WhatsApp (35)
- Tags
- Reports

Fig A.2 – Autopsy overall device results



```
vol30 (userdata: 4075520-15269847)
    $OrphanFiles (62)
    $Unalloc (6)
    anr (3)
    app (19)
    app-asec (2)
    app-lib (2)
    app-private (2)
    audio (2)
    backup (7)
    camera (2)
    connectivity (2)
    dalvik-cache (4)
    data (209)
        com.android.backupconfirm (5)
        com.android.bluetooth (5)
        com.android.browser (6)
        com.android.browser.provider (5)
        com.android.calendar (6)
```

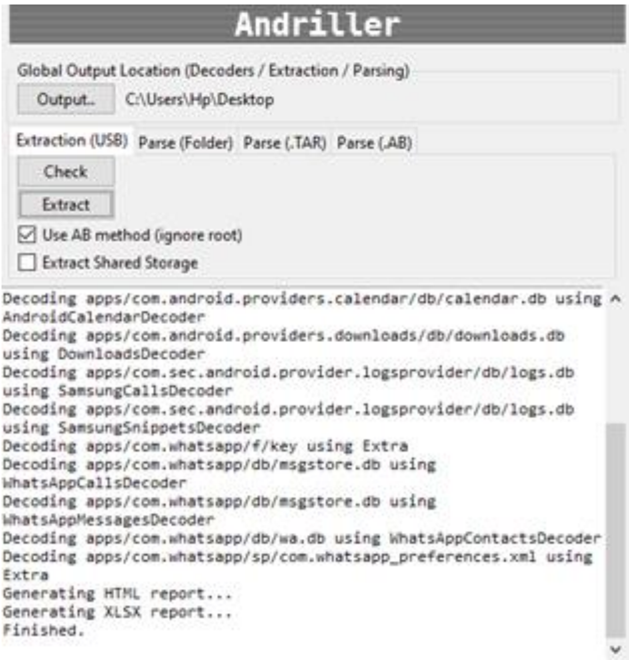
Fig A.3– Autopsy device volume and data navigation



```
com.whatsapp (11)
    app_minidumps (2)
    app_phenotype_file (4)
    cache (21)
    databases (41)
    files (66)
    lib-main (6)
    no_backup (4)
    shared_prefs (41)
com.wsomacp (7)
com.wssnps (6)
com.wssyncmldm (8)
csv.file.reader (8)
media (2)
org.simalliance.openmobileapi.service (5)
org.telegram.messenger (8)
    cache (5)
    databases (4)
    files (36)
    no_backup (3)
    shared_prefs (23)
```

Fig A.4– Autopsy social media application navigation

APPENDIX B – ANDRILLER REPORT



Global Output Location (Decoders / Extraction / Parsing)

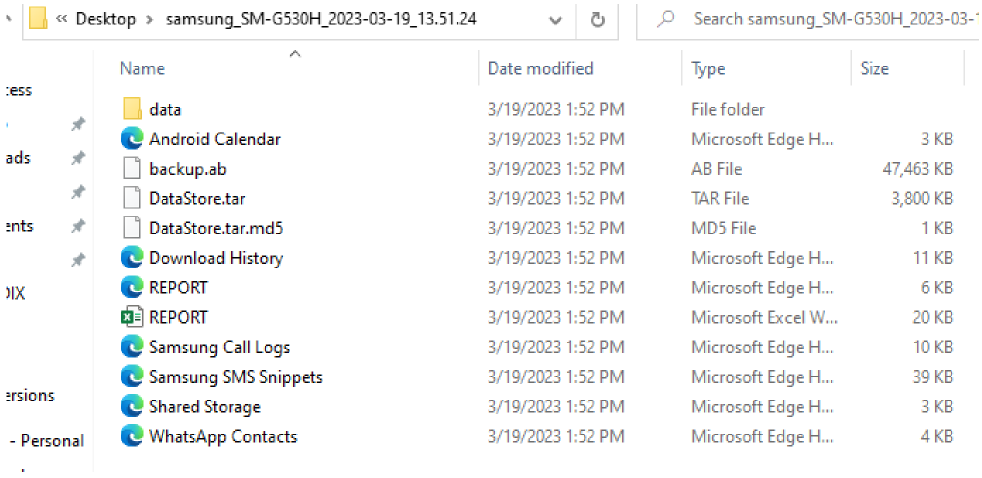
Output.. C:\Users\Hp\Desktop

☑ Use AB method (ignore root)

□ Extract Shared Storage

```
Decoding apps/com.android.providers.calendar/db/calendar.db using
AndroidCalendarDecoder
Decoding apps/com.android.providers.downloads/db/downloads.db
using DownloadsDecoder
Decoding apps/com.sec.android.provider.logsprovider/db/logs.db
using SamsungCallsDecoder
Decoding apps/com.sec.android.provider.logsprovider/db/logs.db
using SamsungSnippetsDecoder
Decoding apps/com.whatsapp/f/key using Extra
Decoding apps/com.whatsapp/db/msgstore.db using
WhatsAppCallsDecoder
Decoding apps/com.whatsapp/db/msgstore.db using
WhatsAppMessagesDecoder
Decoding apps/com.whatsapp/db/wa.db using WhatsAppContactsDecoder
Decoding apps/com.whatsapp/sp/com.whatsapp_preferences.xml using
Extra
Generating HTML report...
Generating XLSX report...
Finished.
```

Fig B.1– Andriller logical image extraction


« Desktop › samsung_SM-G530H_2023-03-19_13.51.24
Search samsung_SM-G530H_2023-03-
:ess
ads
ents
)IX
ersions
- Personal

Name	Date modified	Type	Size
data	3/19/2023 1:52 PM	File folder	
Android Calendar	3/19/2023 1:52 PM	Microsoft Edge H...	3 KB
backup.ab	3/19/2023 1:52 PM	AB File	47,463 KB
DataStore.tar	3/19/2023 1:52 PM	TAR File	3,800 KB
DataStore.tar.md5	3/19/2023 1:52 PM	MD5 File	1 KB
Download History	3/19/2023 1:52 PM	Microsoft Edge H...	11 KB
REPORT	3/19/2023 1:52 PM	Microsoft Edge H...	6 KB
REPORT	3/19/2023 1:52 PM	Microsoft Excel W...	20 KB
Samsung Call Logs	3/19/2023 1:52 PM	Microsoft Edge H...	10 KB
Samsung SMS Snippets	3/19/2023 1:52 PM	Microsoft Edge H...	39 KB
Shared Storage	3/19/2023 1:52 PM	Microsoft Edge H...	3 KB
WhatsApp Contacts	3/19/2023 1:52 PM	Microsoft Edge H...	4 KB

Fig B.2– Andriller overall extraction results

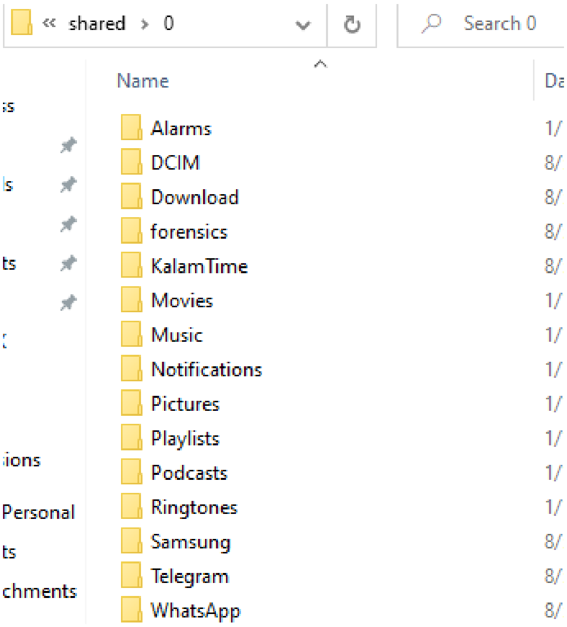


Fig B.3– Andriller device data navigation

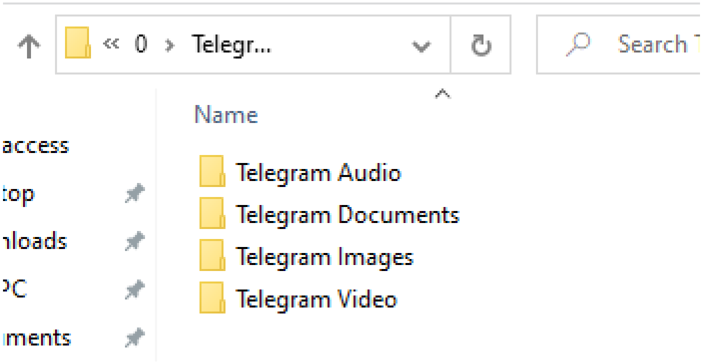
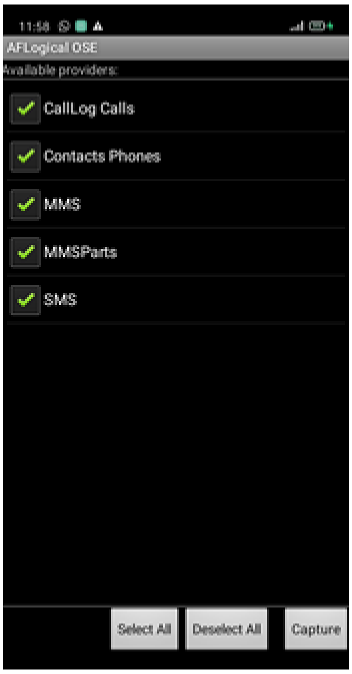


Fig B.3– Andriller application data

APPENDIX C – AFLOGICAL REPORT



AFLogical OSE

Available providers:

☑ CallLog Calls

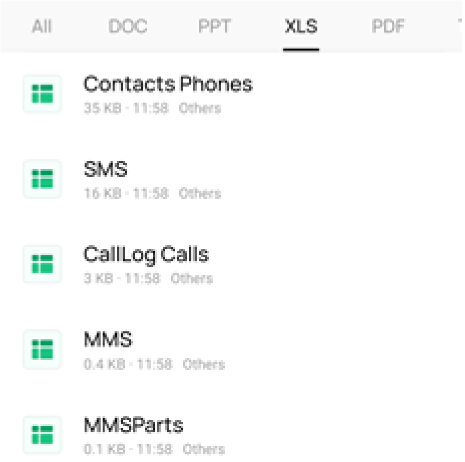
☑ Contacts Phones

☑ MMS

☑ MMSParts

☑ SMS

Fig C.1– AFLogical image acquisition



Contacts Phones
35 KB · 11:58 Others

SMS
16 KB · 11:58 Others

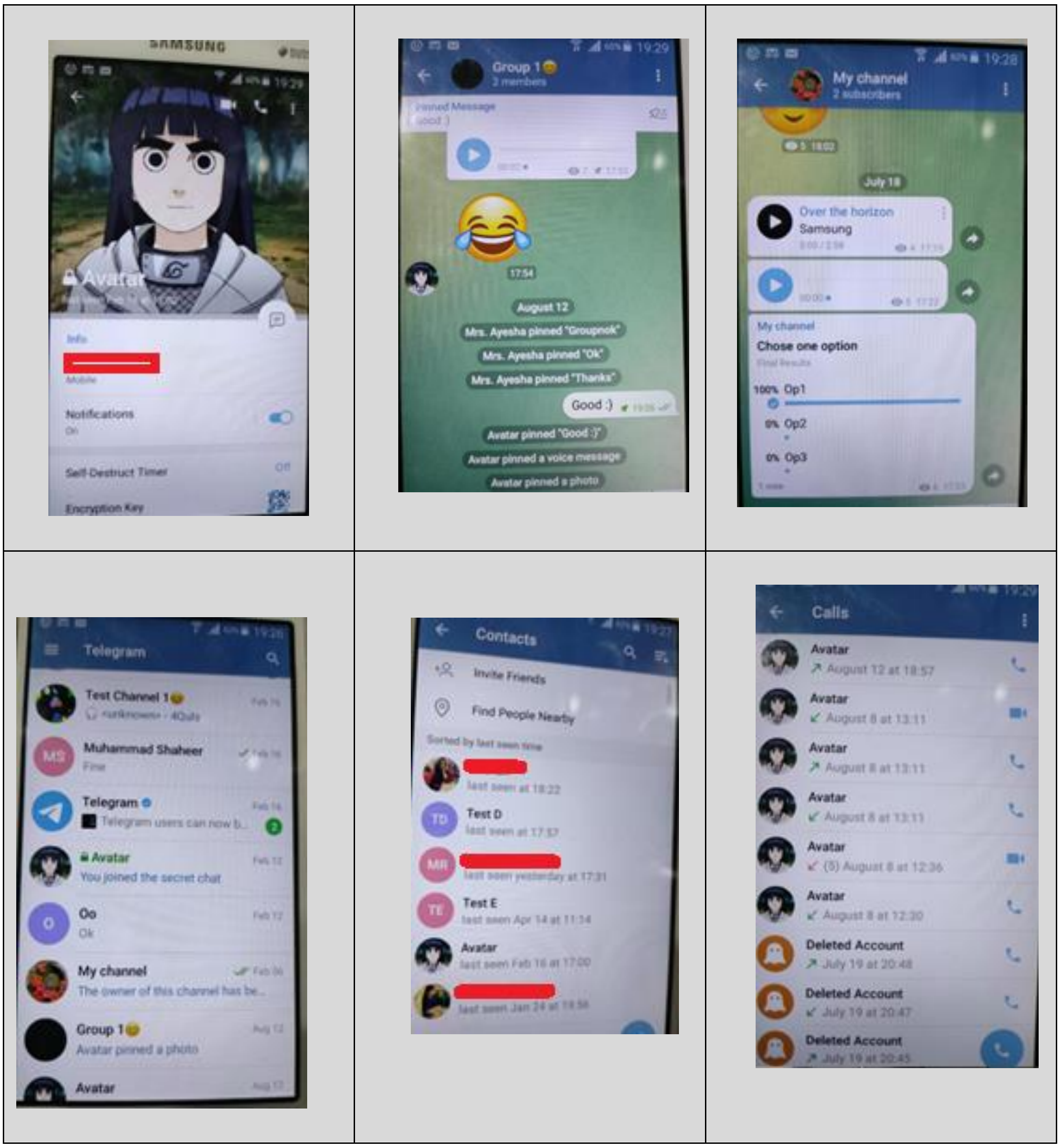
CallLog Calls
3 KB · 11:58 Others

MMS
0.4 KB · 11:58 Others

MMSParts
0.1 KB · 11:58 Others

Fig C.2– AFLogical device data extraction results

APPENDIX D – SOCIAL MEDIA APPLICATION ACTIVITIES



Avatar

Info

[redacted]

Mobile

Notifications

On

Self-Destruct Timer Off

Encryption Key

Group 1

2 members

Pinned Message

Good :)

17:54

August 12

Mrs. Ayesha pinned "Groupnok"

Mrs. Ayesha pinned "Ok"

Mrs. Ayesha pinned "Thanks"

Good :)

Avatar pinned "Good :)"

Avatar pinned a voice message

Avatar pinned a photo

My channel

2 subscribers

July 18

Over the horizon

Samsung

My channel

Chose one option

Final Results

100% Op1

0% Op2

0% Op3

Telegram

Test Channel 1		Feb 16
Muhammad Shaheer	Fine	Feb 16
Telegram	Telegram users can now b...	Feb 16
Avatar	You joined the secret chat	Feb 12
Oo	Ok	Feb 12
My channel	The owner of this channel has be...	Feb 06
Group 1	Avatar pinned a photo	Aug 12
Avatar		Aug 12

Contacts

Invite Friends

Find People Nearby

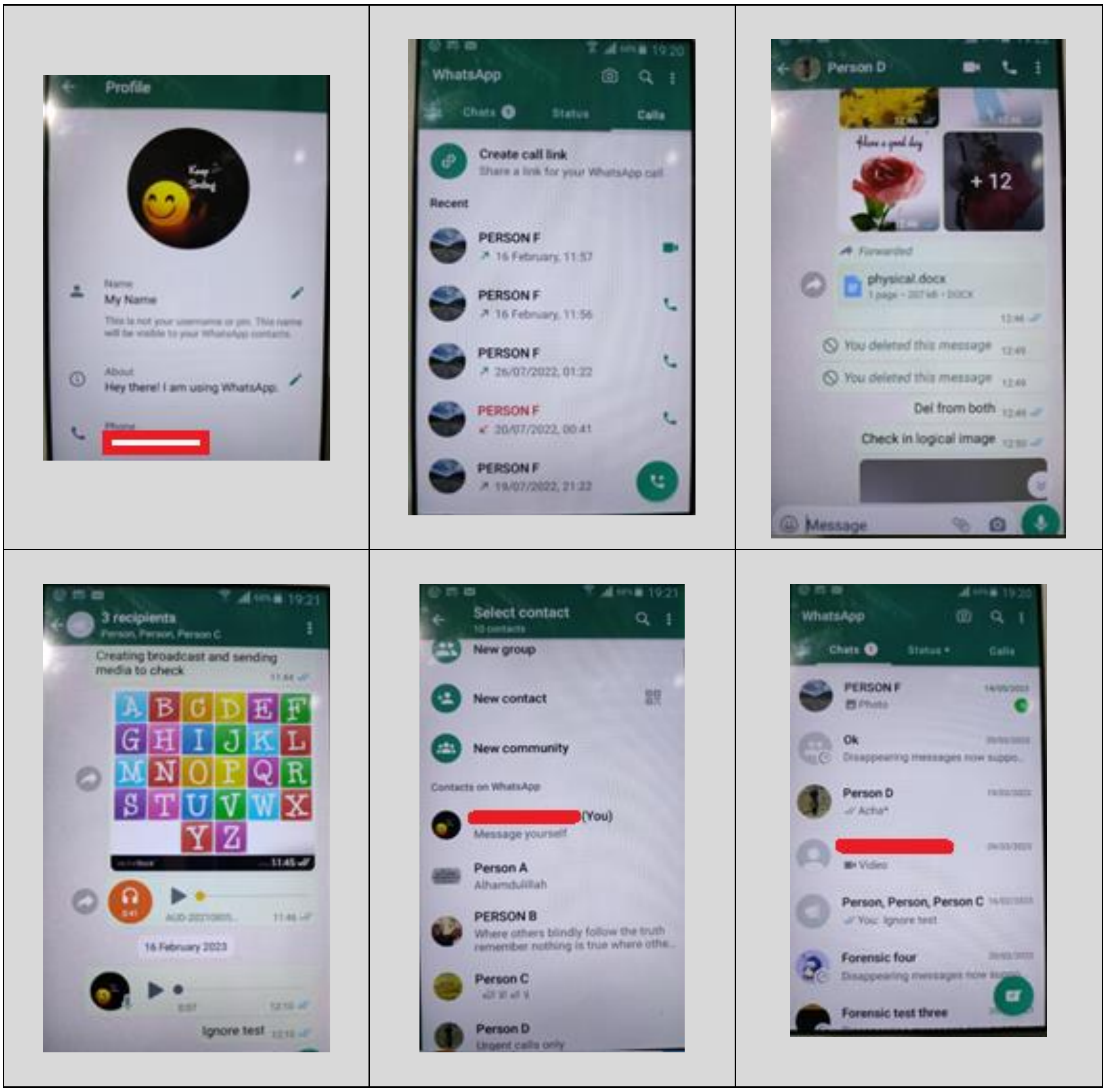
Sorted by last seen time

[redacted]	last seen at 18:22
Test D	last seen at 17:57
[redacted]	last seen yesterday at 17:31
Test E	last seen Apr 14 at 11:14
Avatar	last seen Feb 16 at 17:00
[redacted]	last seen Jan 24 at 18:56

Calls

Avatar	↗ August 12 at 18:57
Avatar	↙ August 8 at 13:11
Avatar	↗ August 8 at 13:11
Avatar	↙ August 8 at 13:11
Avatar	↙ (5) August 8 at 12:36
Avatar	↙ August 8 at 12:30
Deleted Account	↗ July 19 at 20:48
Deleted Account	↙ July 19 at 20:47
Deleted Account	↗ July 19 at 20:45

Fig D.1—Telegram activities



Profile

Name
My Name
This is not your username or pin. This name will be visible to your WhatsApp contacts.

About
Hey there! I am using WhatsApp.

Phone
[redacted]

WhatsApp

Chats Status Calls

Create call link
Share a link for your WhatsApp call

Recent

PERSON F
↗ 16 February, 11:57

PERSON F
↗ 16 February, 11:56

PERSON F
↗ 26/07/2022, 01:22

PERSON F
↙ 20/07/2022, 00:41

PERSON F
↗ 19/07/2022, 21:22

Person D

Have a good day

+ 12

Forwarded

physical.docx
1 page · 207 kB · DOCX
12:46

You deleted this message 12:49

You deleted this message 12:49

Del from both 12:49

Check in logical image 12:50

Message

3 recipients
Person, Person, Person C

Creating broadcast and sending media to check 11:44

A B C D E F
G H I J K L
M N O P Q R
S T U V W X
Y Z

11:45

AUD-2023 11:46

16 February 2023

12:10

Ignore test 12:10

Select contact
10 contacts

New group

New contact

New community

Contacts on WhatsApp

[redacted](You)
Message yourself

Person A
Alhamdulillah

PERSON B
Where others blindly follow the truth remember nothing is true where othe...

Person C

Person D
Urgent calls only

WhatsApp

Chats Status Calls

PERSON F
Photo

Ok
Disappearing messages now suppo...

Person D
Acha*

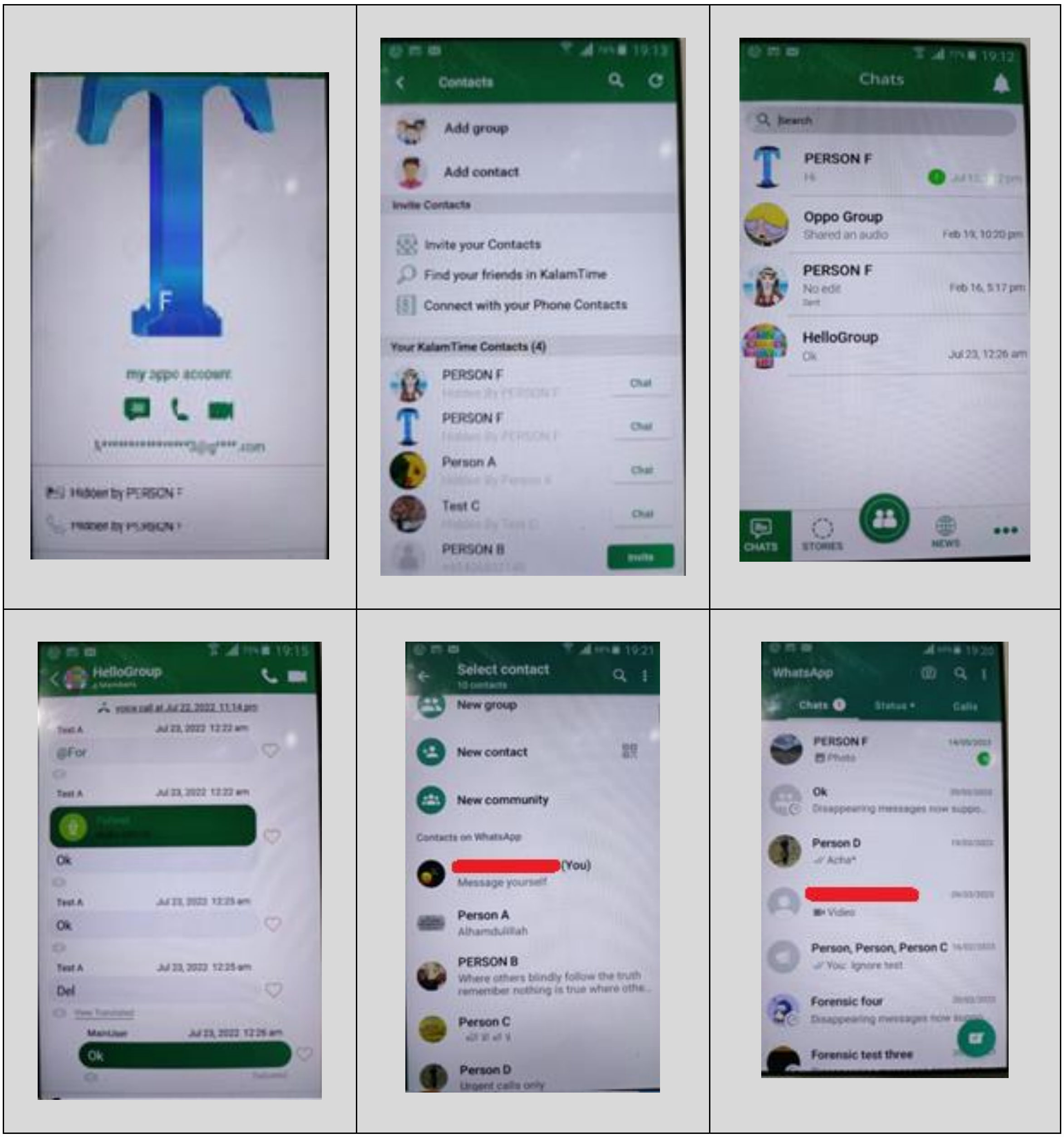
[redacted]
Video

Person, Person, Person C
You: Ignore test

Forensic four
Disappearing messages now suppo...

Forensic test three

Fig D.2—Whatsapp activities



my oppo account

t***************@g***.com

Hidden by PERSON F

Hidden by PERSON F

Contacts

Add group

Add contact

Invite Contacts

Invite your Contacts

Find your friends in KalamTime

Connect with your Phone Contacts

Your KalamTime Contacts (4)

PERSON F — Chat

PERSON F — Chat

Person A — Chat

Test C — Chat

PERSON B — Invite

Chats

Search

PERSON F — Hi

Oppo Group — Shared an audio — Feb 19, 10:20 pm

PERSON F — No edit — Sent — Feb 16, 5:17 pm

HelloGroup — Ok — Jul 23, 12:26 am

CHATS STORIES NEWS

HelloGroup

voice call at Jul 22, 2022 11:14 pm

Test A — Jul 23, 2022 12:22 am

@For

Test A — Jul 23, 2022 12:22 am

Ok

Test A — Jul 23, 2022 12:25 am

Ok

Test A — Jul 23, 2022 12:25 am

Del

View Translated

MainUser — Jul 23, 2022 12:26 am

Ok

Select contact

New group

New contact

New community

Contacts on WhatsApp

[redacted] (You) — Message yourself

Person A — Alhamdulillah

PERSON B — Where others blindly follow the truth remember nothing is true where othe…

Person C

Person D — Urgent calls only

WhatsApp

Chats Status Calls

PERSON F — Photo

Ok — Disappearing messages now suppo…

Person D — Acha*

[redacted] — Video

Person, Person, Person C — You: ignore test

Forensic four — Disappearing messages now su…

Forensic test three

Fig D.3—Kalamtime activities