



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

MSc in Cybersecurity and Digital Forensics

**Module: Research Methods and Professional
Development**

Module Code: ACFA7004

Assessment Component 1: Research Proposal

Lecturer: Dr Suresh Shanmugasundaram

Title of Proposal:

Forensic Analysis of Social Messaging Platforms on an
Android Device

Student Name: Habibur Rahman

Student Number: 2428138

Date of Submission: 1st May 2026

Table of Contents

List of Figures	3
List of Tables	3
1. Introduction	4
1.1 Context and Background	4
1.2 Research Problem	5
1.3 Research Aim and Objectives	6
1.3.1 Aim	6
1.3.2 Objectives	6
1.4 Significance of the Research	6
2. Literature Review	7
3. Research Design and Methodology	9
3.1 Research Design	9
3.2 Research Methods and Materials	9
3.2.1 Methods	9
3.2.2 Materials	10
4. Expected Outcome	12
5. Timeline	13
6. References	14
7. Appendices	15

List of Figures

Figure 1: Research Design Model 9

Figure 2: Data Analysis Process 10

Figure 3: Estimated Timeline (Gantt Chart) 13

List of Tables

Table 1: Evidential Integrity and Investigator Awareness Matrix 5

Table 2: Research Problem Summary 5

Table 3: Forensic Tools Overview 11

Table 4: Project Impact and Stakeholder Benefits 13

1. Introduction

This proposal focuses on the forensic analysis of social messaging applications on Android devices. It explores how digital evidence may be recovered and why differences between applications matter in forensic investigation. The next section explains the context and background of the proposed study.

1.1 Context and Background

Social messaging platforms are now one of the main ways people communicate in both their personal and professional lives. Apps such as WhatsApp, Telegram, Signal, Facebook Messenger, and Snapchat are used by billions of people every day, and the messages shared on them range from ordinary conversations to highly private information. However, these platforms are also sometimes used for criminal activities such as cybercrime, fraud, extremist communication, and drug-related offences [1]. Because of this, forensic investigators need a clear understanding of how these applications store and protect data, as this has become an essential part of digital forensic practice.

Android is the most widely used mobile operating system in the world, so it is the platform most often encountered in digital forensic investigations. This makes Android-focused forensic methods especially important in practice. Research found that communication and social media applications have some of the most changeable data structures on mobile devices [1]. In simple terms, this means that useful evidence can be difficult to recover, and even a small app update may change where data is stored or how it can be accessed. This issue, often described as schema drift, was also highlighted [2], who showed that changes in app database structures can reduce the accuracy and reliability of forensic tools.

This is a serious issue because evidence taken from messaging applications is now commonly used in criminal investigations and court cases. For that evidence to be useful, it must be collected properly, remain reliable, and preserve its integrity. For this reason, investigators need to understand what kinds of data can be recovered, where that data is stored, and which acquisition methods are most suitable [3].

The table below outlines the main reasons why this topic is important in cybersecurity and digital forensics.

Aspect	Explanation
Evidential integrity	Digital evidence must be reliable and legally admissible in court
Investigator awareness	Understanding what data can be recovered informs investigative strategy
Public safety	Forensic evidence of messaging activity helps convict offenders
Tool development	Research identifies gaps in current forensic

	software and methods
--	----------------------

Table 1: Evidential Integrity and Investigator Awareness Matrix

1.2 Research Problem

The central research problem is the lack of clear comparative forensic guidance for investigators examining multiple social messaging applications on modern Android devices. Each app stores data in its own way. For example, Telegram uses a mix of cloud and local storage, while its secret chats are kept in a separate encrypted part of the database [4]. Signal is even more difficult from a forensic point of view because it uses end-to-end encryption and stores messages in an SQLCipher-encrypted database, meaning that recovery often depends on whether the passphrase can be obtained from the device memory [5]. Because of these differences, there is no single forensic tool or acquisition method that works equally well for every app, even though investigators often need to analyse several of them on the same device.

Another challenge is the issue of schema drift, where app updates change the database structure that forensic tools rely on to extract and interpret data [1]. This means that a tool that works well on one version of an app may not work properly on a newer version, which creates a real risk of missing important evidence. Research shows that this is not a minor or occasional issue, but an ongoing problem that requires tools to be checked and validated whenever app versions change [2].

Disappearing messages make the situation even more difficult. This feature is now common in apps such as WhatsApp, Signal, and Telegram. Although these messages are meant to remove themselves after a set time, previous research has shown that traces can sometimes still be recovered, especially if the relevant database pages have not yet been overwritten [4]. However, whether recovery is possible depends a lot on what happens on the device after deletion, so collecting the data quickly is often very important.

Issue	Consequence
Messaging apps store forensic evidence in databases [6]	Investigators need to know where and how to find it
Encryption and disappearing messages limit recovery [7]	Some evidence may be permanently lost
Each app stores data differently [8]	No single method works for all apps
Existing research focuses on single apps or versions [6][8]	Limited practical guidance for real-world investigations

Table 2: Research Problem Summary

1.3 Research Aim and Objectives

1.3.1 Aim

This research proposes to investigate the forensic traces left by social messaging applications on Android devices and to explore how those traces can be identified, extracted, and interpreted during a digital forensic investigation.

1.3.2 Objectives

To achieve this aim, the study has four main objectives.

The first is to identify the types of evidence that messaging applications leave behind on an Android device in a controlled environment, such as messages, media files, call logs, and deleted content [2].

The second is to use both commercial and open-source forensic tools, including FTK, Cellebrite UFED, Cellebrite Physical Analyzer, ADB, SQLite Browser, and Autopsy, to extract and analyse the artefacts produced by each application [8].

The third objective is to compare the recovery of evidence across different messaging platforms to determine which applications provide more recoverable artefacts and which are more resistant to forensic examination [1][7].

The final objective is to examine how encryption and disappearing message features affect the recovery process, and to identify the situations in which deleted or temporary data may still be recovered [1][4].

1.4 Significance of the Research

This research addresses several practical needs within digital forensics. For investigators, the study will provide evidence-based guidance on the most appropriate forensic tools and acquisition methods for different messaging platforms on Android devices. This need has been recognised for some time; earlier work showed that evidence recovery varies widely between applications and that no single forensic approach works reliably in all cases [7]. By examining multiple platforms side by side, this study helps clarify where existing methods are effective and where they fall short. It also responds to recent calls within the digital forensics community for a more consistent way of evaluating artefact recovery across secure messaging applications [9].

The research is also relevant to legal professionals who rely on digital evidence in criminal proceedings. A clear understanding of the technical limits of forensic extraction, particularly in relation to end-to-end encryption and disappearing messages, is essential to avoid misinterpreting missing data as a lack of user activity. In addition, this study contributes to an

area of the academic literature where comparative, cross-platform analysis using a standardized approach remains limited [8].

2. Literature Review

One of the earliest and most important studies in this area is the forensic analysis of WhatsApp on Android, which helped establish a basic approach for examining messaging applications by analysing SQLite databases, cache files, and shared preferences to recover chat history, contact information, and media content [6]. The study showed that even in earlier versions of WhatsApp, a large amount of useful forensic evidence could be recovered from the device. At that time, the application's local database was not encrypted, which made forensic extraction much easier than it is today [6].

A comparative study of twenty popular Android messaging applications showed that evidence recoverability varies significantly across platforms, particularly when encrypted databases are used on unrooted Android devices.[7]. They found that message content could be reconstructed from sixteen of them, showing that recoverability varies significantly across platforms. They also demonstrated that device forensics and network forensics can complement each other, as each method may reveal artefacts that the other misses. This comparative perspective is particularly relevant to the present study, although their work was carried out before the major Android security changes introduced in more recent versions of the operating system.

The problem of identifying SQLite evidence on Android devices is an automated tool for recognising and extracting SQLite database files created or modified by messaging apps [10] . This work is important because SQLite files do not always have clear file extensions, which means they can sometimes be missed by standard forensic tools. By using both file extensions and binary headers, FORC improves the detection of relevant database files. This is particularly useful for the manual verification stage of the current study.

Signal has received particular attention in forensic research because of its strong privacy protections. A method for acquiring and decrypting Signal backup files on Android, showing that chats and attachments can be recovered when the backup passphrase is available or can be derived [5]. This work also supports earlier findings that Signal's use of the Signal Protocol and SQLCipher encryption makes standard logical acquisition far less effective. In many cases, physical acquisition or memory analysis is needed to recover meaningful evidence. Also showing that even when message content cannot be recovered from the device, network analysis can still reveal useful metadata such as communication timing, traffic volume, content type, and server infrastructure [11].

The issue of disappearing messages has also been examined in previous studies. Investigating Signal, Wickr, and Threema, all of which support timer-based ephemeral messaging, and found that traces of deleted content can sometimes still be recovered from SQLCipher database pages if those pages have not yet been overwritten [4] . These findings show that disappearing

messages are not always completely removed from a forensic perspective, but the opportunity to recover them is usually limited and depend heavily on device activity after deletion. This makes the timing of evidence collection especially important.

A major development in the field came with analysing 320 application versions across several messaging platforms [1]. Their study identified schema drift, meaning changes in database structure after app updates, as one of the biggest challenges to reliable forensic analysis. They showed that these changes can cause forensic tools to misread databases or miss evidence entirely. This concern was later reinforced by the fact that even well-established commercial tools can fail when their internal database definitions are not updated to match newer app versions [2].

The most comprehensive overview of the field is ACM Computing Surveys' systematic review [9]. They concluded that widespread end-to-end encryption has changed the focus of secure messaging forensics. Rather than intercepting communication content, investigators now need to concentrate more on identifying and recovering device-level artefacts. They also argued that the field would benefit from a unified and regularly updated framework for evaluating evidence recovery across secure messaging platforms. The current study responds directly to that need by using a structured comparative approach across three applications within a reproducible methodology.

Research also provides a useful recent contribution by applying the NIST framework to the forensic analysis of Android messaging applications [8]. Their study combines network traffic analysis with device artefact examination, offering a practical structure that fits well with the methodology of the present research. Similarly, a study on WhatsApp, Telegram, and Instagram in a virtual Android environment showed that deleted data may still leave traces in local cache files or remain accessible through server-side storage, depending on the platform [12]. This highlights the importance of understanding both device-level and platform-level storage behaviour when reconstructing evidence.

Overall, the literature shows a clear and consistent gap. Much of the existing research focuses on a single application or a single Android version. There is still limited comparative research that tests multiple tools across multiple messaging platforms on recent Android versions, especially Android 12 to 14, where file-based encryption and scoped storage have introduced new forensic challenges. In addition, although schema drift is now recognised as a serious issue, its effect on day-to-day forensic tool reliability is still being explored. The recovery of disappearing message artefacts also remains insufficiently understood, particularly under different post-deletion conditions.

3. Research Design and Methodology

3.1 Research Design

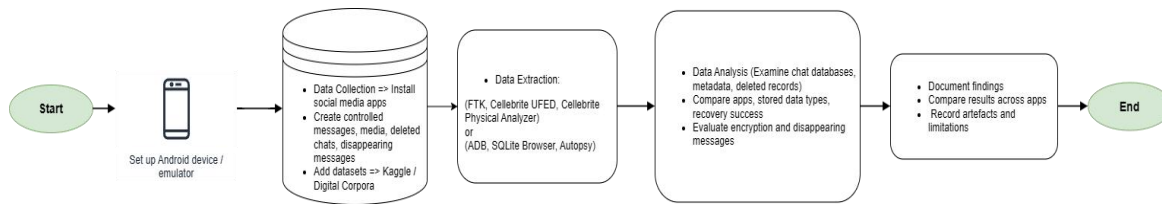


Figure 1: Research Design Model

Follow the details of an experimental forensic case-study approach carried out in a controlled laboratory setting. This design is suitable, as it enables the researcher to examine various acquisition methods across selected messaging applications, then compare the artefacts retrieved in each scenario. Conducting the study in a controlled environment also increases the reliability of the experiment, limiting external influences like physical device model differences or user behavior [8].

The NIST Digital Forensics Framework, described by NIST Special Publication 800-101 Rev. 1, breaks down mobile forensics into four important phases: preservation, acquisition, examination, and reporting [3]. This framework provides the basis to help ensure that research within this area is conducted in accordance with established forensic practice and thus should remain relevant to real-world casework investigations [8].

All experiments would be done on test devices and specific test accounts. At no point will real user data be viewed or processed. The testbed can only be conducted in truly isolated environments, not integrated with live networks. All generated data will be held on encrypted media and subsequently deleted at the project's end to conform with institutional policy on data retention.

3.2 Research Methods and Materials

3.2.1 Methods

Data analysis process (In short):

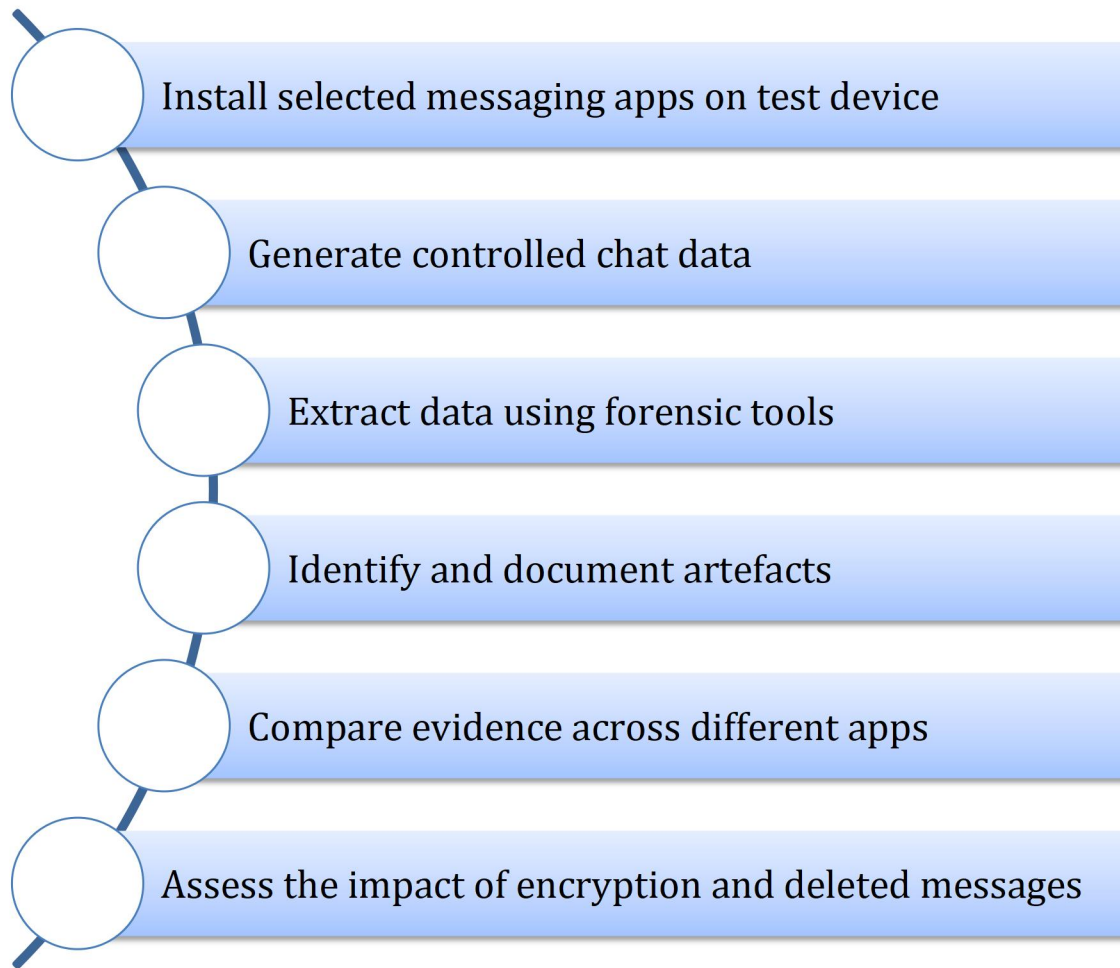


Figure 2: Data Analysis Process

The analysis will examine six categories of artefacts: message content, timestamps, sender and recipient identifiers, media files, call logs, and deleted data. Each category will be assessed across applications and acquisition methods to determine the completeness and reliability of evidence recovery. The findings will be recorded in an artefact recovery matrix and checked against the timestamped activity log created during the test scenarios. To protect the integrity of the evidence, SHA-256 hash verification will be applied at each stage of acquisition in line with the procedures set out in NIST SP 800-101 Rev. 1 [3].

3.2.2 Materials

The project is concerned with selected social messaging applications (WhatsApp, Telegram, Signal, Facebook Messenger, and Snapchat), chosen with the advice of the supervisor based on what are relevant mobile forensic topics at this moment. The platforms where forensic analysis can be performed will be chosen based on their popularity and the different types that provide forensic challenges. WhatsApp keeps a huge volume of data stored locally in its contacts database, which can often be read and decrypted under the right conditions, forensics-wise,

even on non-full-rooted devices [6]. Telegram data is stored in a mix of local and cloud storage, with secret chats stored separately as encrypted [4]. Because it uses end-to-end encryption and stores its local data in an SQL Cipher-encrypted database, Signal is typically harder to analyze; usually, a passphrase must be recovered from device memory before the contents can be viewed [5].

The practical part of the study will be performed on a current version of Android, either on an Android device or in an emulator. Controlled user actions will be designed and executed throughout each application. Such activities as sending and receiving instant text messages, sharing photos and audio files, voice calls, deleting individual messages and conversations, disappearing messages, where the feature is available [4]. Timestamps will be recorded for every activity so that the collected evidence can be compared with the original generation.

The acquisition and analysis stages may use both commercial forensic tools and open-source forensic tools. The table below details the categories of tools and the corresponding subset of tools that were chosen for this study.

Type	Tools
Commercial	FTK (Forensic Toolkit), Cellebrite UFED, Cellebrite Physical Analyzer [8]
Open Source	ADB (Android Debug Bridge), SQLite Browser, Autopsy [6]

Table 3: Forensic Tools Overview

Cellebrite UFED will be used to carry out both logical and file system acquisition from the test device. After the data has been collected, Cellebrite Physical Analyzer will be used to parse and examine the recovered artefacts. FTK will provide an additional layer of verification and support keyword searching across the acquired images. As an open-source tool, Autopsy will be used to cross-check findings and to manually inspect SQLite database files and Write-Ahead Log (WAL) entries, where deleted records may remain for a short time before being overwritten [6]. ADB and SQLite Browser will also be used for lower-level inspection of application folders and database files, allowing the findings from commercial tools to be checked more closely. In cases where SQLite files do not have normal file extensions, the FORC tool developed by Ashawa and Ogwuche may be used as an additional utility to help identify them [10].

The test data will be created directly on the device using a set of controlled scenarios. To make the data more realistic while keeping the study reproducible, public forensic datasets from Digital Corpora and Kaggle will also be used where appropriate [10]. In addition, network traffic generated during the test scenarios will be captured to support analysis. This follows the approach used in earlier studies, which showed that network evidence can sometimes provide useful information when device-level artefacts are limited or encrypted [7][11].

4. Expected Outcome

The principal outcome of this research will be a comparative artefact recovery matrix that evaluates the extent to which each messaging application yields recoverable evidence under different forensic tools and acquisition methods. The main outcome of this research will be a comparative artefact recovery matrix showing how each messaging application performs when examined using different forensic tools and acquisition methods. This matrix is intended to help forensic investigators decide which approach is most suitable when dealing with a particular application, and it responds directly to the need for clearer practical guidance in this area [9].

Based on previous studies, WhatsApp is expected to provide the most complete range of recoverable artefacts during file system extraction because of its local SQLite database structure and the fact that tools such as Cellebrite UFED and Autopsy have already been shown to work effectively with it [6]. Signal is likely to be the most difficult application to analyse because of its strong end-to-end encryption and SQL Cipher-protected local database, although some level of recovery may still be possible through memory analysis or backup decryption methods [5]. Telegram is expected to fall somewhere in between, as some of its data is stored locally while other content remains in the cloud, and secret chat data is stored in encrypted form [4].

The study is also expected to show that schema drift affects the reliability of forensic tools across different app versions, which is consistent with findings from more recent research [1][2]. This would be important for both investigators and tool developers, as it highlights the need to regularly validate forensic tools against newer versions of messaging applications. In relation to disappearing messages, the study is expected to find that some residual artefacts may still be recoverable for a short period after deletion, although this is likely to depend on how quickly the device is acquired and how much activity takes place after the messages disappear [4].

A second outcome of the study will be a set of practical recommendations for investigators, together with a proposed standard operating procedure for the forensic analysis of Android messaging platforms. At the same time, the limitations of the research need to be recognised. The findings will apply only to Android devices and cannot automatically be extended to iOS. The study also relies on data generated in a controlled lab environment rather than real case data, which may reduce how closely the results reflect real-world investigations. In addition, because messaging applications are updated regularly, the findings will only remain valid for the versions examined in this study.

Stakeholder	Benefit
Forensic investigators	Practical guidance on where and how to find evidence from messaging apps on Android
Digital forensics community	Better understanding of evidence recovery across different platforms [7][8]
Tool developers	Identification of gaps in forensic software, including schema drift handling [1][2]

Legal professionals	Clear account of the technical limitations of digital evidence from messaging apps [9]
---------------------	--

Table 4: Project Impact and Stakeholder Benefits

5. Timeline

The project timeline is estimated as follows:

Gantt Chart

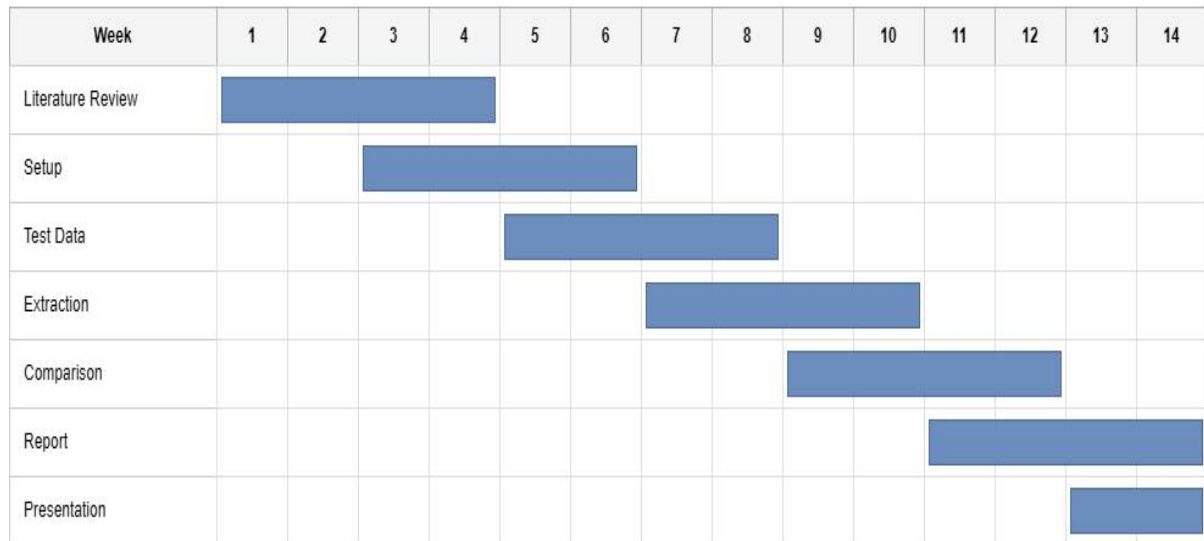


Figure 3: Estimated Timeline (Gantt Chart)

- **Weeks 1–4:** Literature review

Review recent studies on Android messaging app forensics and identify the main research gap.

- **Weeks 3–6:** Set up the device, tools, and test environment

Prepare the Android device or emulator, install the apps, and set up the forensic tools.

- **Weeks 5–8:** Create and organize test data

Generate sample activities such as messages, media sharing, voice calls, deleted chats, and disappearing messages.

- **Weeks 7–10:** Carry out data extraction

Use the selected forensic tools to extract data from the device and collect available artefacts.

- **Weeks 9–12:** Compare findings across the apps and tools

Analyze the recovered evidence and compare how each app and tool performs.

- **Weeks 11–14:** Write the report

Organize the findings and write the research proposal in a clear academic structure.

- **Weeks 13–14:** Prepare the presentation

Create the slides and summarise the key points of the proposed study clearly.

6. References

- [1] R. F. Abu Hweidi, et al., "Forensics Investigation on Social Media Apps and Web Apps Messaging in Android Smartphone," *2023 International Conference on Smart Applications, Communications and Networking (SmartNets)*, 2023. doi: 10.1109/SmartNets58706.2023.10216267.
- [2] A. M. Azahari, A. Oliveri and D. Balzarotti, "Resilience of forensic evidence acquisition under database schema drift," *Forensic Science International: Digital Investigation*, vol. 56, pp.302059, 2026. doi: 10.1016/j.fsidi.2026.302059. Available: <https://www.sciencedirect.com/science/article/pii/S2666281726000168>
- [3] R. Ayers, et al., "Guidelines on Mobile Device Forensics (Draft) Recommendations of the National Institute of Standards and Technology," 2013. Accessed: 30 April 2026. [Online]. <https://doi.org/10.6028/NIST.SP.800-101r1>
- [4] J. Son, et al., "Forensic analysis of instant messengers: Decrypt Signal, Wickr, and Threema," *Forensic Science International: Digital Investigation*, vol. 40, -01-31 2022. doi: 10.1016/j.fsidi.2022.301347.
- [5] S. Krishnapriya, V. S. Priyanka and S. S. Kumar, "Forensic Extraction and Analysis of Signal Application in Android Phones," 2021-12-21. doi: 10.1109/fabs52071.2021.9702702.
- [6] C. Anglano, "Forensic analysis of WhatsApp Messenger on Android smartphones," *Digital Investigation*, vol. 11, no. 3, pp.201–213, 2014. doi: 10.1016/j.diin.2014.04.003. Available: <https://www.sciencedirect.com/science/article/pii/S1742287614000437>
- [7] D. Walnycky, et al., "Network and device forensic analysis of Android social-messaging applications," *Digital Investigation*, vol. 14, pp.S77–S84, 2015. doi: 10.1016/j.diin.2015.05.009. Available: <https://www.sciencedirect.com/science/article/pii/S1742287615000547>
- [8] R. Bramesta Kusumadewa and Z. Sari, "Comparative Analysis of Forensic Digital Evidence on Android Smartphone based Instant Messaging Using NIST Framework,"

- [9] A. R. Onik, et al., "A Systematic Literature Review of Secure Instant Messaging Applications from a Digital Forensics Perspective," *ACM Comput. Surv.*, vol. 57, no. 9, -05-07 2025. doi: 10.1145/3727641.
- [10] E. Daraghmi, et al., "Forensic Operations for Recognizing SQLite Content (FORC): An Automated Forensic Tool for Efficient SQLite Evidence Extraction on Android Devices," *Applied Sciences*, vol. 13, no. 19, -09-27 2023. doi: 10.3390/app131910736.
- [11] A. Afzal, et al., "Encrypted Network Traffic Analysis of Secure Instant Messaging Application: A Case Study of Signal Messenger App," *Applied Sciences*, vol. 11, no. 17, -08-24 2021. doi: 10.3390/app11177789.
- [12] D. Millatina, E. H. Gunawan and B. Sugiantoro, "Forensic Analysis of WhatsApp, Instagram, and Telegram on Virtual Android Device," 2024-04-29. doi: 10.1109/isdfs60797.2024.10527308.

7. Appendices

Appendix A: Test Device and Environment

- Android device or emulator running Android 13 or later.
- A mid-range Android phone may be used if a physical device is available.
- Separate test accounts are created for each messaging app.
- No real user data is used in the study.

Appendix B: Forensic Tools

- **FTK** – used for disk imaging and keyword search.
- **Cellebrite UFED** – used for logical and file system extraction.
- **Cellebrite Physical Analyzer** – used to examine extracted artefacts.
- **ADB** – used for direct device access and file retrieval.
- **Autopsy** – used for verification and SQLite analysis.
- **DB Browser for SQLite** – used to inspect database files and WAL entries.
- **FORC** – used to detect SQLite files without normal extensions [10].

Appendix C: Data Sources

- Test data will mainly be created through the controlled scenarios on the device.
- Digital Corpora may be used as supporting forensic data. Kaggle datasets may also be used where needed.