Mobile Forensics for Fraud Cases on the Telegram Platform

Muh Rusman[a,1], Ramdan Satra [a,2]; Huzain Azis [a,3]

[a] *Universitas Muslim Indonesia, Jl. Urip Sumoharjo km.05, Makassar dan 90231, Indonesia*

[1] *rmuhrmuh@gmail.com;* [2] *ramdan@umi.ac.id;* [3] *huzain.azis@umi.ac.id*

ARTICLE INFORMATION

Received : 10 – 12 – 2025
Revised : 12 – 12 – 2025
Published : 22 – 04 – 2026

Keywords:
Digital Forensics
Telegram
Android
JPG File
NIST SP 800-86
FTK Imager

ABSTRACT

The use of the Telegram application as a communication medium allows the exchange of image files that have the potential to become digital evidence, but in some cases the perpetrator deletes the files to eliminate digital traces. This study aims to analyze and prove the ability of the digital forensic process in finding and recovering deleted JPG image files on the Android-based Telegram application so that they can be used as valid digital evidence. The research method refers to the NIST SP 800-86 standard which includes the stages of collection, examination, analysis, and reporting, with the data acquisition process using the logical acquisition method through the Android Debug Bridge (ADB) without root access as well as analysis using FTK Imager and verification of data integrity through SHA-256 hash values. The results of the study show that JPG image files that have been deleted from the Telegram application can still be found and recovered from the internal storage media of Android devices in intact condition, have relevant metadata, and consistent hash values, so they are declared valid as digital evidence.

I. Introduction

Developments in information and communication technology have driven the increasing use of instant messaging applications as a primary means of communication. One such application widely used by Indonesians is Telegram. Despite its convenience, Telegram is also frequently misused as a medium for cybercrime, particularly fraud. This is reflected in several cases in Indonesia, including a fraud case through a Telegram group using the "paid mission" method, which resulted in a loss of Rp 50 million for a woman in Palembang [1], and a case of fraud disguised as freelance work through Telegram, which resulted in a loss of Rp 31 million for the victim [2]. In both cases, the perpetrators communicated with the victims via messages and Telegram groups, then deleted the conversations after the transactions were completed. This action causes the communication evidence to no longer be visible on the application interface, thus complicating the digital investigation process, although it is still possible that digital artifacts may remain on the device's storage system.

Previous research has shown that digital forensics plays a crucial role in uncovering digital evidence in cybercrime cases. Research conducted by academics at the Muslim University of Indonesia (UMI) confirmed that the implementation of the National Institute of Standards and Technology (NIST) framework is capable of maintaining the integrity and validity of digital evidence through the collection, examination, analysis, and reporting stages [3]. Other research from the UMI academic environment also concluded that the NIST method is effective in the acquisition and analysis of digital evidence on various storage media, particularly in maintaining the consistency and validity of examination results [4]. On the other hand, research focusing on the Telegram application shows that deleted text messages are generally difficult to recover due to the security and encryption systems implemented by the application [5]. However, the study also revealed that digital artifacts in the form of media files and Telegram application

caches can still be found on Android devices and have the potential to serve as relevant digital evidence in forensic processes [6].

Based on these issues and previous research, this study focuses on the recovery and analysis of media artifacts in the form of image files (JPG) in the Telegram application. This study uses a logical acquisition method without rooting the Android device, followed by an imaging process using FTK Imager, which refers to the NIST framework. The main difference between this study and previous studies lies in the focus of the analysis, which is directed only at image files stored in the Telegram application cache directory. This study does not aim to recover text messages or the application's internal database, but rather confirms that remaining image artifacts can still serve as valid digital evidence and can be forensically accounted for through a hash verification process.

II. Method

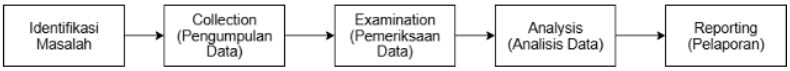

Figure 1 Research Chart

1. Problem Identification Determining the focus of research on online arisan fraud cases via WhatsApp, with special attention to messages deleted by the perpetrator.
2. Collection (Data Collection) At this stage, digital data is acquired from the Android device using FTK Imager. This tool was chosen because it is able to create complete image files and maintain the integrity of the evidence.
3. Examination (Data Examination) The acquired data is then examined to find important digital artifacts, such as the WhatsApp database file msgstore.db and the crypt12/crypt14 backup files.
4. The recovered database was analyzed using SQLite Browser to extract deleted conversations. The analysis results were verified using hashes (MD5/SHA1) to ensure no data changes occurred. This method proves effective for analyzing WhatsApp group conversations.
5. Reporting: All investigation results are presented in a forensic report, which includes procedures, findings, and recovered conversation evidence. Standardized reporting is essential for the legal validity of digital evidence.

III. Results and Discussion

A. Identification

The identification phase is the initial stage in the digital forensics process, which aims to determine the investigation's needs and identify evidence relevant to the case. Based on the identification results, it was discovered that the primary evidence was an Android smartphone belonging to the perpetrator with the Telegram application installed.

At this stage, the type of data to be analyzed was also determined: JPG image files suspected of having been sent or received via the Telegram application. Data storage location identification was conducted to identify potential directories where the image files could be stored. The identification results indicated that the Telegram files were stored on the device's internal storage, accessible through the Android external storage directory.

Figure 2. Perpetrator's Cell Phone

The suspect was then identified on a personal smartphone device, which was reported as an online arisan fraud on the Telegram app. The victim's report included screenshots of the perpetrator's crime, which were then linked to applicable laws.

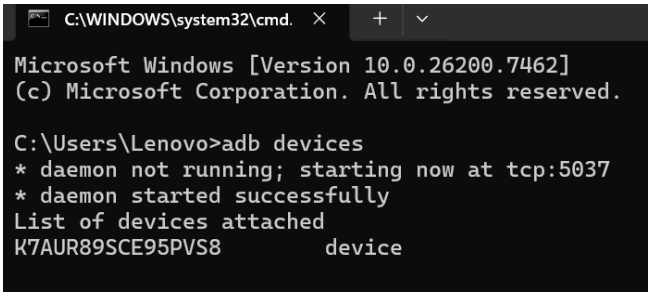

Figure 3. Perpetrator Device

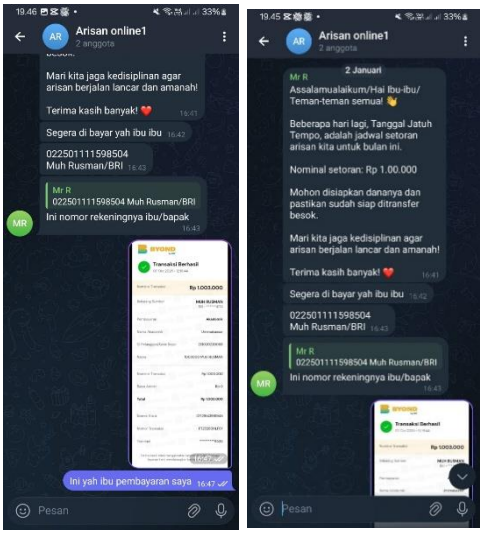

Figure 4. Screenshot Evidence of Conversation on the Victim's Device

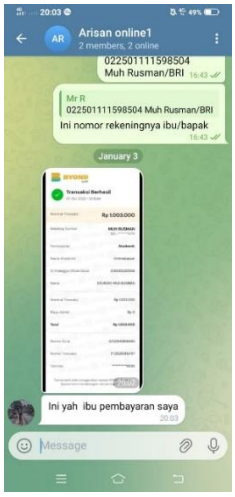

Figure 5. Screenshot Evidence of the Perpetrator Before

Figure 6. After Deleting the JPG Evidence

Based on these images, a clear link can be seen between communication activities and the perpetrator's attempts to delete digital evidence. The first image shows screenshots of conversations via the Telegram app, from both the victim's and the perpetrator's devices, containing communication related to the transaction and the sending of proof of payment in the form of an image file (JPG). These screenshots show the conditions before and after the perpetrator deleted the image file from the

conversation, indicating an attempt to erase the digital footprint after the transaction was completed. Furthermore, the second image shows screenshots of the perpetrator's Instagram account before and after deleting feed posts. The change in the number of posts to zero indicates that the perpetrator not only deleted evidence of the conversation on Telegram but also deleted visual content on the Instagram account used as a medium for offering the message. All of this evidence corroborates the fact that the perpetrator intentionally deleted digital artifacts on multiple platforms to eliminate any connection to the fraud experienced by the victim.

B. Collection

The Collection phase is carried out to collect digital data from the perpetrator's device without changing the original data. This process uses the logical acquisition method with the help of the Android Debug Bridge (ADB) tool, which was chosen because it does not require root access and thus minimizes the risk of data changes on the device. Acquisition begins with device detection using the adb devices command, then copying the Telegram directory from the device's internal storage using the adb pull /sdcard/Telegram command to the evidence folder on the investigator's computer. All acquired data is stored in a special directory as part of documentation and chain of custody maintenance.

```
C:\Users\Lenovo>cd evidence_telegram
```

Figure 7. Calling a folder that has been created

Next, create a folder using CMD. After creating the folder, create a command to call the folder, namely cd evidence_telegram.

```
C:\Users\Lenovo\evidence_telegram>adb shell ls /sdcard | findstr Telegram
Telegram
```

Figure 8. Ensuring the Telegram directory is available

After creating a folder, enter the stage of ensuring whether the Telegram directory is available or not.

```
C:\Users\Lenovo\evidence_telegram>adb pull /sdcard/Telegram C:\evidence_telegram
/sdcard/Telegram/: 8 files pulled, 0 skipped. 1.3 MB/s (125350 bytes in 0.093s)
```

Figure 9. Retrieving Telegram data

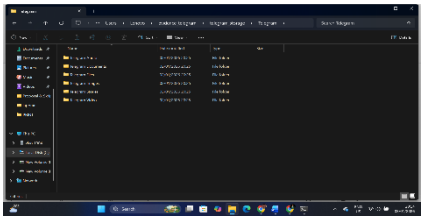

Figure 10. Telegram Data Results

After ensuring that the Telegram directory is available, now enter the stage of retrieving data from Telegram which contains Telegram Audio, Telegram Documents, Telegram Files, Telegram Stories, and Telegram Video.

C. Examination

The Examination phase is conducted after the data acquisition process is complete, with the aim of examining and tracing the logical acquisition data. The examination begins by opening the acquisition folder on the investigator's computer, then exploring the Telegram directory structure using a file explorer and FTK Imager. At this stage, the investigator traces the Telegram/Images storage path to identify digital artifacts in the form of image files.

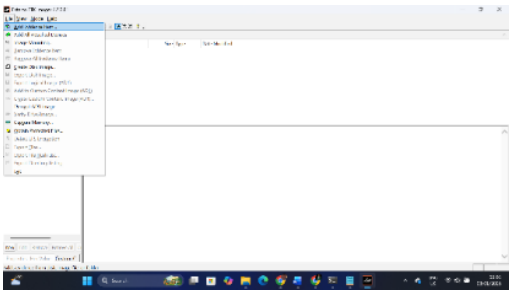

Figure 11. Adding Digital Evidence

Once the application is ready to use, the next step is to add digital evidence to FTK Imager via the File → Add Evidence Item menu. At this stage, the "Contents of a Folder" option is selected because the data being analyzed is the result of a logical acquisition. The Telegram acquisition folder is then loaded into FTK Imager, allowing the entire directory structure to be directly explored without altering the original data.

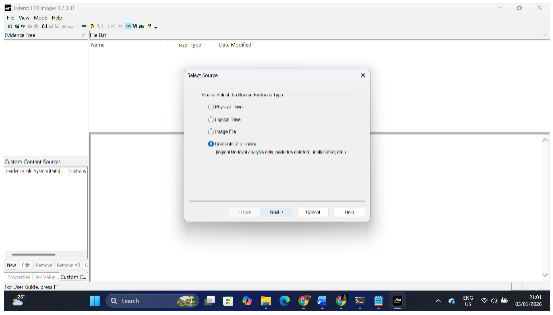

Figure 12. Telegram Directory Structure Browsing

After successfully loading the evidence, a search of the Telegram directory structure was conducted using the Evidence Tree panel. The search was conducted systematically by opening the main Telegram folder and available subfolders. This step aimed to understand Telegram's data storage structure and identify potential locations for storing digital artifacts relevant to the research.

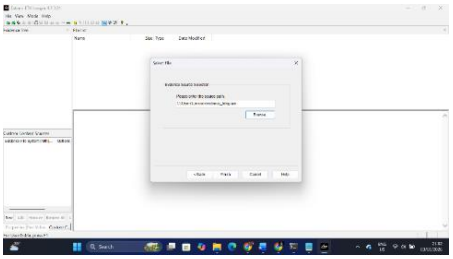

Figure 13. Folder Telegram Images

Based on the search results, a Telegram Images folder was identified, which became the primary focus of the analysis. This folder was examined because it potentially stores image files previously used in Telegram communications. The existence of this folder indicates that even if a user deletes images from the app, digital artifacts may still be stored on the device's storage.

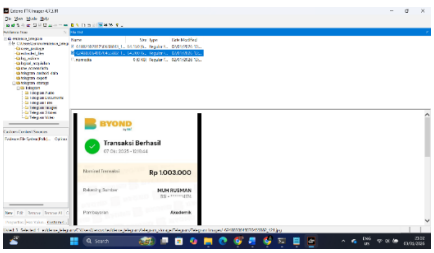

Figure 14. JPG Image File

In this step, JPG image files contained in the Telegram Images folder are identified. FTK Imager displays a complete file list with basic information such as file names and file sizes. This identification ensures that the files found are relevant digital artifacts and not system or temporary files.

D. Analysis

The analysis phase is the core stage of this research, which aims to analyze the JPG image files recovered in the previous process. The analysis was performed on the logical acquisition files without altering the original data, thus maintaining the authenticity of the evidence. The entire analysis process adhered to the NIST SP 800-86 standard and was carried out systematically.

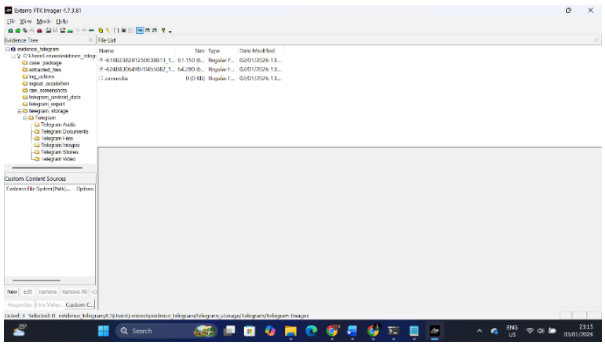

Figure 15. File JPG

The initial step in the analysis phase was to identify JPG image files contained in the Telegram acquisition directory. This identification was performed by searching the Telegram Images folder using FTK Imager. At this stage, the researchers confirmed that the files found were indeed in JPG format and originated from the Telegram directory, thus confirming that they were digital artifacts relevant to the research.

The results of this stage show that several JPG image files were successfully found, even though they had previously been deleted by the perpetrator from the Telegram application display.

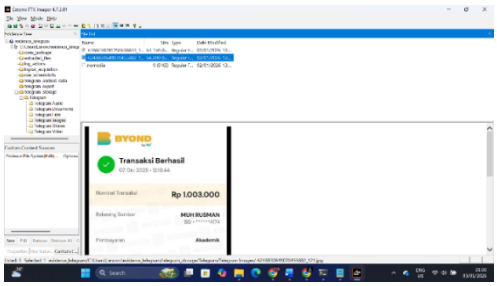

Figure 16. Preview and Validate JPG Files

Once the JPG file has been identified, the next step is to preview the file using the Image Preview feature in FTK Imager. This preview ensures that the image file can still be opened and displayed normally. This step also checks for file corruption.

Based on the preview results, the JPG file can be displayed clearly without any visual damage, so it can be concluded that the file is still intact and worthy of further analysis.

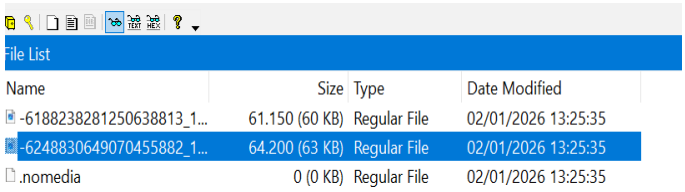

Figure 17. JPG File Metadata Analysis

The next step was to analyze the metadata on the JPG file using FTK Imager. The metadata examined included the creation time, modification time, and file size information. This metadata information is crucial for understanding the chronology of the file's use before it was deleted by the perpetrator.

The metadata analysis results showed that the file's creation and modification times corresponded to communication activity times on the Telegram app. This strengthens the indication that the JPG file had been used and shared via the Telegram app before being deleted.

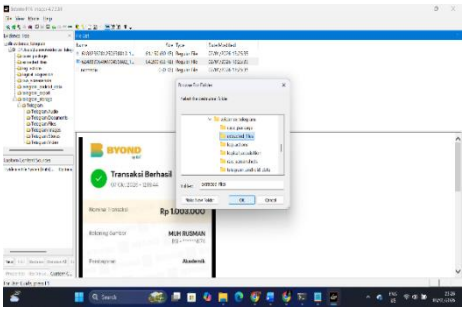

Figure 18. JPG File Extraction

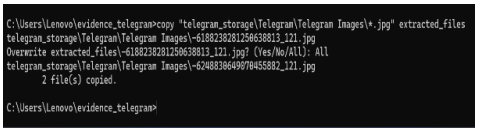

Figure 19. JPG File Analysis

After the files were deemed relevant and intact, the JPG files were extracted from FTK Imager into a separate folder on the investigator's computer. The extraction process was performed using the Export Files feature in FTK Imager so that the analyzed files could be further processed without affecting the original data acquisition.

The extraction was successful, and the JPG files were safely stored in the extracted_files folder, ready for the data integrity verification stage.

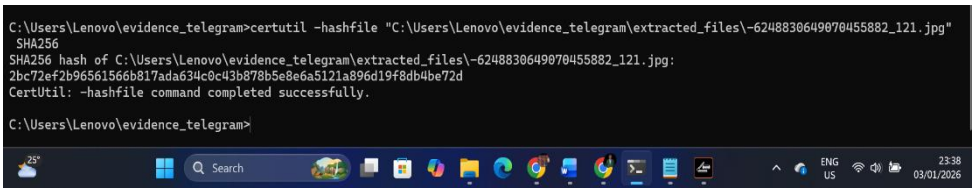

Figure 20. Hash Value Calculation (SHA-256)

The final stage in the analysis process is calculating the JPG file's hash value to maintain the integrity and validity of the digital evidence. The hash calculation was performed using the certutil command via the Command Prompt using the SHA-256 algorithm. This hash value serves as the file's digital identity and is used to ensure that the file has not been altered during the analysis process.

The hash calculation results show that the JPG file's SHA-256 value is consistent and unchanged. This indicates that the image file has not been modified from the time it was extracted until its analysis, thus maintaining the authenticity of the evidence and can be scientifically and legally validated.

Based on the analysis results at this stage, the recovered JPG image file can be opened normally and is undamaged. Metadata examination indicates that the file's time and characteristics match Telegram usage activity. Furthermore, the hash calculation results using the SHA-256 algorithm show consistent values, concluding that the file has not been altered during the analysis process. Therefore, the JPG file is declared valid and can be used as legal digital evidence.

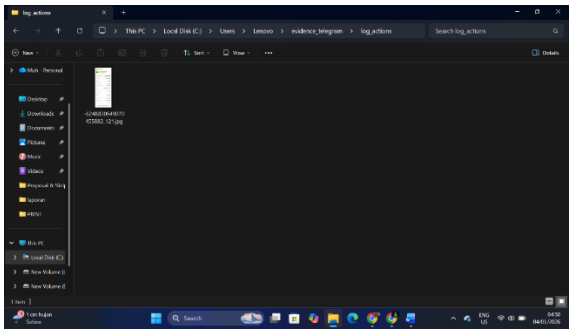

Figure 21. View of the recovered JPG file

The image shows that the recovered JPG image file can be opened and displayed normally, which indicates that the file was not damaged after the deletion and recovery process was carried out.

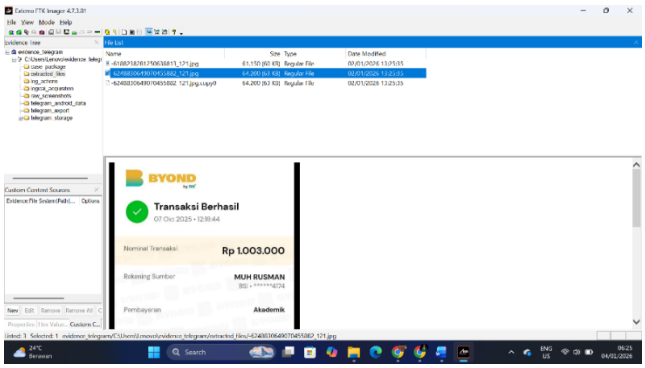

Figure 22. JPG File Metadata in FTK Imager

File metadata shows creation and modification time information relevant to Telegram app usage activity, thus strengthening the file's association with the events under study.

```
C:\Users\Lenovo\evidence_telegram>certutil -hashfile "C:\Users\Lenovo\evidence_telegram\extracted_files\-6248830649070455882_121.jpg"
 SHA256
SHA256 hash of C:\Users\Lenovo\evidence_telegram\extracted_files\-6248830649070455882_121.jpg:
2bc72ef2b96561566b817ada634c0c43b878b5e8e6a5121a896d19f8db4be72d
CertUtil: -hashfile command completed successfully.

C:\Users\Lenovo\evidence_telegram>
```

Figure 4.22 Hash Value Verification Results SHA-256

The results of calculating the hash value using the SHA-256 algorithm show consistent values, which indicates that the file has not changed during the inspection and analysis process.

E. Reporting

The reporting stage is the final stage in the digital forensics process, documenting the entire series of research activities in a systematic and structured manner. At this stage, all the results from each previous stage are compiled into a scientific report so that they can be understood, tested, and justified academically and legally.

This final stage of the digital forensics evidence analysis based on the NIST method is the reporting stage, which presents the results of the analysis conducted in the previous stages. This includes a description of the evidence obtained during the evidence acquisition process, as shown in Table 4.3.

The discussion in this study focuses on the digital forensics process of the Telegram application on Android devices, specifically the recovery of JPG image files deleted by the perpetrator. All research stages were conducted systematically, adhering to the NIST SP 800-86 standard, from the identification process to reporting the results. By implementing a logical acquisition method without root access, this study emphasizes the importance of maintaining data authenticity and integrity throughout the investigation. The results show that even though image files have been deleted from

the Telegram application, the digital artifacts can still be found on the device's storage media, analyzed using FTK Imager, and validated through hash calculation. This finding proves that deleted data is not always permanently lost and still has strong evidentiary value if appropriate digital forensic handling is carried out.

1. Digital Forensic Methods

   This research applies digital forensic methods referring to the NIST SP 800-86 standard which includes the stages of identification, collection, examination, analysis, and reporting, so that the research process is carried out systematically and structured.

2. Data Acquisition Techniques

   The data collection process is carried out using logical acquisition via Android Debug Bridge (ADB) without root access, with the aim of maintaining the authenticity of the data and minimizing the risk of changes to the perpetrator's device.

3. Discovered Digital Artifacts

   The main digital artifact found was a JPG image file stored in the Telegram Images directory, even though the file had been deleted from the Telegram application by the perpetrator.

4. File Inspection and Analysis

   The found JPG files were examined using FTK Imager to view the directory structure, file contents, and metadata, to ensure that the files were intact and could be accessed normally.

5. Data Integrity Verification

   To ensure the validity of the evidence, a SHA-256 hash value was calculated on the extracted files. The hashing results showed consistent values, indicating that the files were unchanged during the inspection and analysis process.

6. Digital Evidence Value

   Based on the analysis results, the JPG file was proven to be related to communication activities on the Telegram application and can be declared as valid digital evidence.

IV. Conclusion

Based on the results of a digital forensic study conducted on the Telegram application on the perpetrator's Android device, it can be concluded that JPG image files that have been deleted by the user can still be recovered through the application of appropriate digital forensic methods. The data acquisition process was carried out using the logical acquisition method with the help of Android Debug Bridge (ADB), so that data can be obtained without root access and without changing the original data on the device. The results of the examination and analysis showed that the JPG image file was successfully found in the Telegram storage directory and could be opened intact, and contained metadata relevant to Telegram application activity based on analysis using FTK Imager. The data integrity verification process through the calculation of the SHA-256 hash value showed consistent results, thus proving that the file was not changed during the acquisition and analysis process and was declared valid as legal digital evidence. This study also proved that deleting files through the Telegram application does not necessarily permanently remove data from the device's storage media, as long as the data has not been overwritten, digital artifacts still have the potential to be recovered through digital forensic processes. Therefore, the application of the NIST SP 800-86 standard in this study has been proven to be able to produce a systematic, structured, and scientifically and legally accountable investigation process. As a suggestion, further research is recommended to analyze non-media digital artifacts such as Telegram databases (SQLite), activity logs, and conversation metadata to obtain a more comprehensive context of events, and it is hoped that the results of this study can be a reference in handling real digital forensic cases involving instant messaging applications, especially Telegram, for law enforcement officers and digital forensic practitioners.

Thank-you note

The author expresses his gratitude to God Almighty for His grace and blessings, enabling him to successfully complete this final project. He would like to thank Mr. Ramdan Satra and Mr. Huzain Azis, his supervisors, for their guidance, direction, and input throughout the process of preparing this research. He would also like to thank all lecturers, academic staff, family, and colleagues for their prayers, support, and motivation, which enabled him to successfully complete this research.

BIBLIOGRAPHY

[1] S. A. - and A. Zubaidi, "Wanita Ini Jadi Korban Penipuan di Misi Grup Telegram, Uang Rp 50 Juta Raib," detikSumbagsel. Accessed: Dec. 20, 2025. [Online]. Available: https://www.detik.com/sumbagsel/hukum-dan-kriminal/d-7759233/wanita-ini-jadi-korban-penipuan-di-misi-grup-telegram-uang-rp-50-juta-raib?utm_source=chatgpt.com

[2] D. Fadilla, "Lagi, Penipuan Berkedok Freelance di Palembang Rugikan Korban Rp 31 Juta," detikSumbagsel. Accessed: Dec. 20, 2025. [Online]. Available: https://www.detik.com/sumbagsel/hukum-dan-kriminal/d-7331159/lagi-penipuan-berkedok-freelance-di-palembang-rugikan-korban-rp-31-juta

[3] Aidil Wijaya Kusuma, Erick Irawadi Alwi, and Ramdaniah Ramdaniah, "Analisis Bukti Digital Pada Media Penyimpanan Flash Disk Menggunakan Metode National Institute Of Standards And Technology (NIST)," *Cyber Secur. dan Forensik Digit.*, vol. 7, no. 1, pp. 18–24, 2024, doi: 10.14421/csecurity.2024.7.1.4345.

[4] H. Supardin, R. Satra, M. Arfah, and M. Foey, "Comparison Analysis of Digital Forensic Tools on Instagram Messenger using The National Institute of Standards and Technology (NIST) Method," vol. 6, no. 1, pp. 65–75, 2022.

[5] D. M. Syafitri and F. Fachri, "Analisis forensik digital telegram pada android untuk," vol. 10, no. 1, pp. 41–50, 2025.

[6] A. Raza and M. Bilal Hassan, "Digital Forensic Analysis of Telegram Messenger App in Android Virtual Environment," *Mob. Forensics*, vol. 4, no. 1, pp. 31–43, 2022, doi: 10.12928/mf.v4i1.5537.