Equivalent: Jurnal Ilmiah Sosial Teknik
Volume 8, Issue 2, 477-494
e_ISSN: 2775-0833
https://jurnalequivalent.id/index.php/jequi/index
DOI: doi.org/10.59261/jequi.v8i2.320

Validation of the Harmonized Mobile Forensic Investigation Process Model (HMFIPM) on Android Devices

Mutia Aziza[1*]
Universitas Indonesia, Indonesia

Muhammad Salman[2]
Universitas Indonesia, Indonesia

***Corresponding author:**
Mutia Aziza, Universitas Indonesia, Indonesia. ✉ mutia.aziza@ui.ac.id

Article Info:

Article history:
Received: April 17, 2026
Revised: May 18, 2026
Accepted: May 25, 2026

Keywords:
Mobile Forensic, HMFIPM, UFED Cellebrite dan MD

Abstract

Background: The increasing use of smartphones has been accompanied by the growing misuse of mobile devices in cybercrime, making mobile forensics essential for identifying, acquiring, recovering, and analyzing digital evidence. However, standardized mobile forensic investigation models for field implementation remain limited. The *Harmonized Mobile Forensic Investigation Process Model* (HMFIPM) has been proposed as a structured investigation model, but its empirical implementation in an accredited forensic laboratory environment remains underexplored.
Objective: This study aims to empirically validate the implementation of HMFIPM as a structured process model for Android mobile forensic investigations within an ISO/IEC 17025-accredited Digital Forensics Laboratory.
Methods: This study applied a descriptive and implementation-based approach. Descriptive analysis was conducted through examiner interviews, while implementation analysis was performed by applying the HMFIPM stages to a Samsung SM-A075F device using Full File System extraction with Cellebrite UFED and Android Live extraction with MD.
Results: All HMFIPM stages were successfully implemented and mapped to the mobile forensic workflow in the laboratory environment. The model supported a structured, documented, and evaluable investigation process. Differences in artifact recovery were primarily caused by tool-to-method compatibility and application data architecture rather than by limitations of the HMFIPM model. Cellebrite UFED using Full File System acquisition produced more complete artifacts, while MD using Android Live extraction obtained partial application artifacts.
Conclusion: HMFIPM is feasible as a standardized framework for Android mobile forensic investigation. However, the feedback mechanism requires refinement. This study proposes an additional data acquisition feedback path alongside the existing analysis feedback path, allowing examiners to revisit the acquisition stage when new investigative needs arise.

To cite this article: Aziza, M. & Salman, M. (2026). Validation of the Harmonized Mobile Forensic Investigation Process Model (HMFIPM) on Android Devices. *Equivalent: Jurnal Ilmiah Sosial Teknik*, 8(2), 477-494. https://doi.org/10.59261/jequi.v8i2.320

INTRODUCTION

Indonesia, with a population of 277.7 million people, recorded 370.1 million mobile phone connections (averaging more than one phone per person), 204.7 million internet users, and 191.4 million social media users. Based on data from the Directorate of Cyber Crimes, the number of cybercrimes continues to increase annually, with many cases involving mobile devices as instruments of crime. This condition indicates that mobile devices not only function as communication tools but also serve as important sources of digital evidence requiring

professional and validated forensic handling.

Mobile forensics (MF) is a branch of digital forensics (DF) that focuses on the process of acquiring, recovering, and analyzing data from mobile devices such as smartphones and tablets. This field plays a crucial role in assisting investigators in uncovering digitally stored electronic evidence that can be used in law enforcement processes (Fukami et al., 2021). However, technological advancements, operating system complexity, and variations in extraction methods pose challenges for investigators in maintaining data integrity and ensuring that each stage of the process complies with digital forensic laboratory standards, such as ISO/IEC 17025.

In line with these needs, research conducted by Arafat Al-Dhaqm et al. (2021) proposed the Harmonized Mobile Forensic Investigation Process Model (HMFIPM) as a framework that integrates various structured mobile forensic investigation processes (Banesinh, 2025; Haluszka & Mansour, 2023; Şen & Artuner, 2025). The study recommended that the HMFIPM be tested and validated in real-world contexts to ensure its effectiveness and compatibility with current forensic practices. Based on this recommendation, the present research was conducted to validate the HMFIPM on Android devices in a Digital Forensics Laboratory using two primary extraction tools, Cellebrite UFED and MD, within an ISO/IEC 17025-accredited laboratory environment (Hamad & Eleyan, 2022).

This research is designed to address several primary research questions, namely how the validation process of the Harmonized Mobile Forensic Investigation Process Model (HMFIPM) is implemented on Android devices in a Digital Forensics Laboratory environment, and how the verification results demonstrate the feasibility of the HMFIPM as a standardized mobile forensic investigation process model. In line with these research questions, the general objective of this study is to validate the HMFIPM as a mobile forensic investigation model for Android devices within an ISO/IEC 17025-standardized Digital Forensics Laboratory environment. Specifically, this research aims to assess the applicability of each procedure and stage in the HMFIPM within the context of an actual investigation and to evaluate the consistency and reliability of digital evidence extraction results through the use of two different forensic tools, namely Cellebrite UFED and MD.

The benefit of this research is that it provides empirical validation of the conceptual HMFIPM on Android devices and contributes to narrowing the research gap in Indonesia regarding the validation of mobile forensic investigation models. Meanwhile, the scope of this research is focused on analyzing data extracted from Android devices that have been verified as a ground truth dataset by forensic analysts in a digital forensics laboratory. This research specifically uses a Samsung Android device as the primary object of investigation, with the extraction process conducted using two forensic tools, Cellebrite UFED and MD, to ensure the validity and reliability of the investigation results.

METHOD

The data analysis technique in this study was carried out through a descriptive and implementation-based approach to the application of the Harmonized Mobile Forensic Investigation Process Model (HMFIPM) in mobile forensic investigations of Android devices. Qualitative analysis was conducted based on the results of interviews with examiners and digital forensic investigators at the Digital Forensic Laboratory to obtain information related to mobile forensic investigation practices in the field. This analysis was used to determine the Android device used as a test object, compile the research dataset, select an acquisition method, and understand the implementation of each HMFIPM stage in the digital forensic investigation process. The model implementation analysis was conducted through the application of the HMFIPM stages in the mobile forensic investigation process on the device, where the results of the acquisition and analysis of digital artifacts were used to evaluate the applicability of each HMFIPM stage, identify the dynamics of the investigation process, and assess the need for feedback-based improvements derived from the investigation results obtained during implementation.

Data Collection Techniques

This research applied the Harmonized Mobile Forensic Investigation Process Model (HMFIPM) as a framework for data collection techniques, as shown in the figure 1.

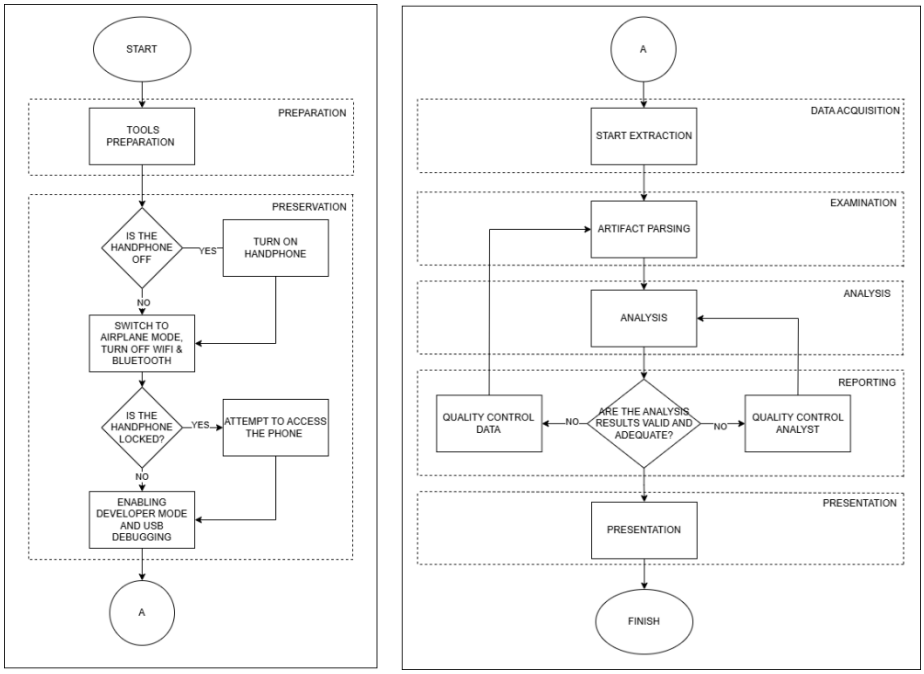


Figure 1. HMFIPM Implementation Flowchart
source: research data

The stages of this research followed the Harmonized Mobile Forensic Investigation Process Model (HMFIPM) workflow, starting with the preparation stage, i.e., preparing the device and forensic investigation environment by ensuring the readiness of the tools and the Android device as the research object. Next, the preservation stage was carried out to maintain the integrity of the evidence through an initial condition assessment of the device, network isolation (Airplane Mode and disabling Wi-Fi and Bluetooth), as well as lawful device access and enabling Developer Options as prerequisites for acquisition. The data acquisition stage was conducted using the physical extraction method to obtain comprehensive data, including both active and residual data. The acquired data were then processed during the examination stage through the parsing of artifacts, such as system logs, metadata, and application artifacts, for structured analysis. The analysis stage focused on interpreting digital artifacts to identify patterns and relevant information based on the ground truth dataset, which was subsequently evaluated to ensure data validity and sufficiency. This process incorporated a feedback mechanism during the reporting stage, namely examination feedback for data quality control and analysis feedback for analyst quality control. The final stage was presentation, i.e., presenting the investigation results in the form of systematic, transparent, and accountable reports and visualizations.

Data Analysis Techniques

The data in this study were analyzed descriptively and interpretatively based on the result of examiner interviews and the implementation of the HMFIPM stages. The analysis focused on assessing the suitability and applicability of HMFIPM in Android mobile forensic investigations, identifying process dynamics during acquisition and analysis, and formulating feedback-based improvements based on the findings obtained during implementation.

RESULTS AND DISCUSSION

Research Results

Simulation of HMFIPM Model Investigation Implementation

The simulation of the HMFIPM model in the Digital Forensics Lab began with implementing the first stage of the HMFIPM model: preparation. Previous research explained that the preparation stage involves isolating the mobile device to achieve a forensically sound state and prevent data alteration on the mobile device. In this study, isolation was performed when the investigator submitted the evidence for extraction to the forensic lab officer on duty at the reception counter. The officer checked the condition of the evidence, ensuring that Airplane Mode was activated and that the SIM and memory cards had been removed to maintain the status quo. The officer then recorded detailed information, physically documented the phone and the time of submission in the chain-of-custody form, prepared a handover report containing the evidence examination number, and issued a receipt letter (STP). Subsequently, the documents and evidence were handed over to the examiner.

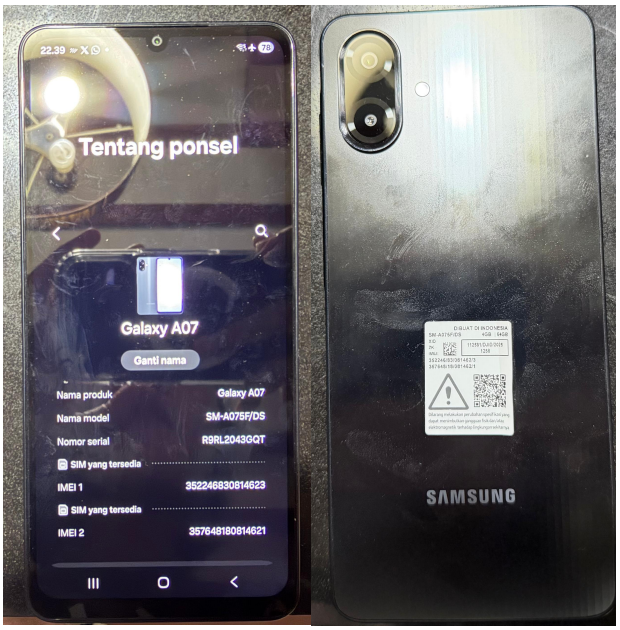


Figure 2. Physical Documentation Results
source: research data

From figure 2, the physical examination results show the product name, model, and serial number, which will be cross-checked by the examiner in the subsequent stage. The next stage is preservation, where previous researchers explained that this stage involves checks to protect the integrity of the mobile device and data. In this study, the preservation stage involved rechecking the documents and evidence using two digital forensic tools to ensure that the data obtained by the officer at the reception counter matched. The examination began by enabling Developer Options and activating USB Debugging to install the digital forensic tool applications on the smartphone, as shown in the figures 3 and 4.

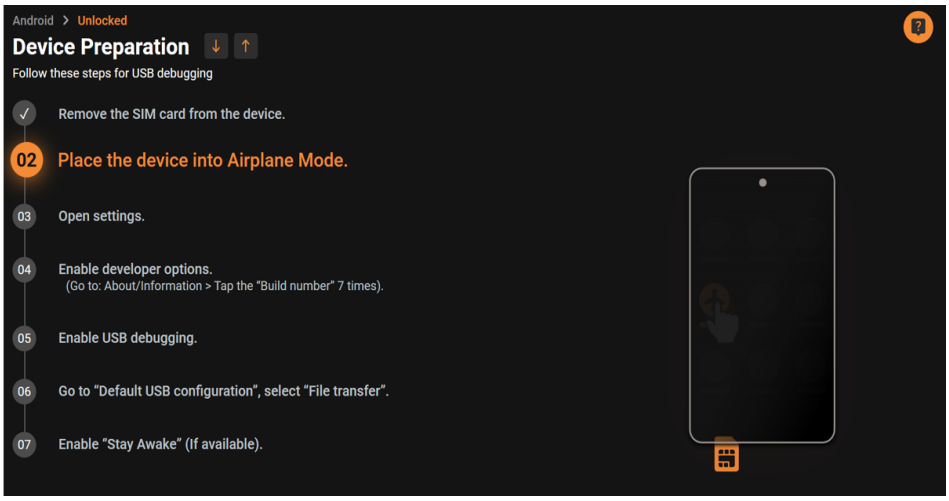


Figure 3. USB debugging activation in Ufed Cellebrite
source: research data

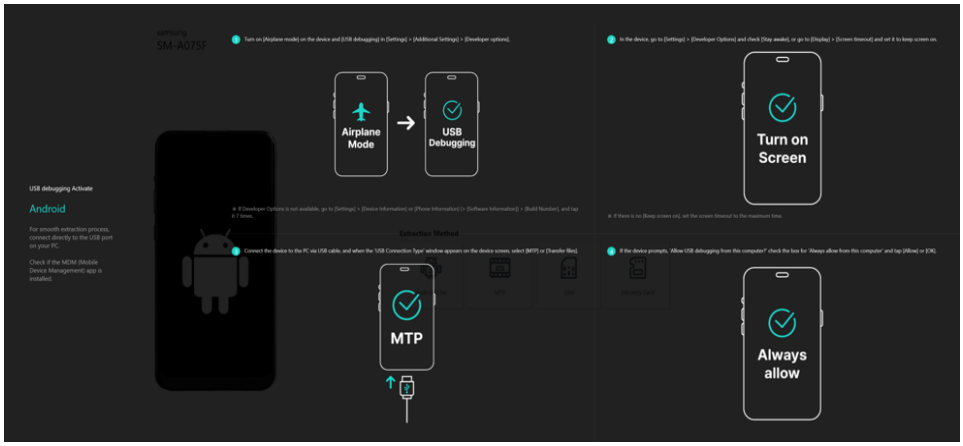


Figure 4. USB debugging activation in MD
source: research data

The figures 3 and 4 show the steps that must be performed by the examiner before data extraction, starting with activating Airplane Mode, turning on the screen, enabling MTP (Media Transfer Protocol), and selecting "Always allow" for all requests on the phone. Both tools follow the same procedure; missing one step results in the inability to proceed to the next step. After all steps have been performed, both tools will automatically detect the phone type. The examiner can use this information to match the data provided by the receiving officer to ensure the integrity of the phone with the examination results, as shown in figure 5.

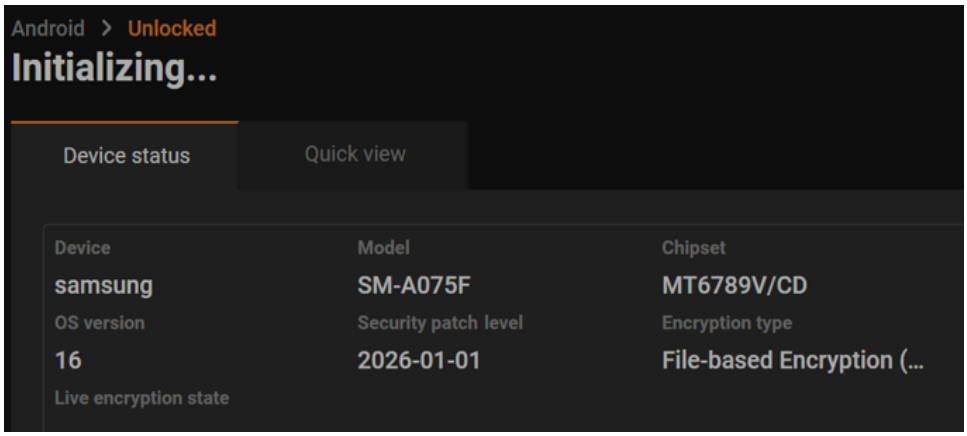


Figure 5. Examination results using Ufed Cellebrite
source: research data

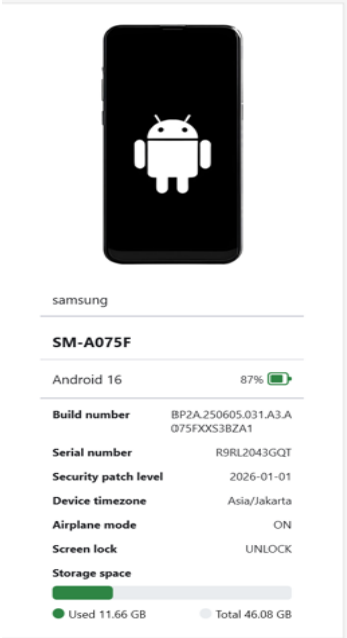


Figure 6. Examination results using MD
source: research data

From Figures 5 and 6, it can be seen that both images show the same information obtained through physical examination and examination using mobile forensic tools, including the product name, model, and serial number. The examination conducted using mobile forensic tools by the examiner is documented in a report and chain of custody to maintain the integrity of the phone data to be examined. The next stage is Data Acquisition. Previous research explained that Data Acquisition is the process of acquiring volatile and non-volatile data from the evidence, consisting of two sub-processes: live acquisition and dead acquisition. Live acquisition is the acquisition process performed while the operating system is still running, whereas dead acquisition is the acquisition process performed when the operating system is powered off. In this study, the examiner performed live acquisition with the phone's initial condition remaining unchanged from the time it was received by the examiner.

Ufed Cellebrite

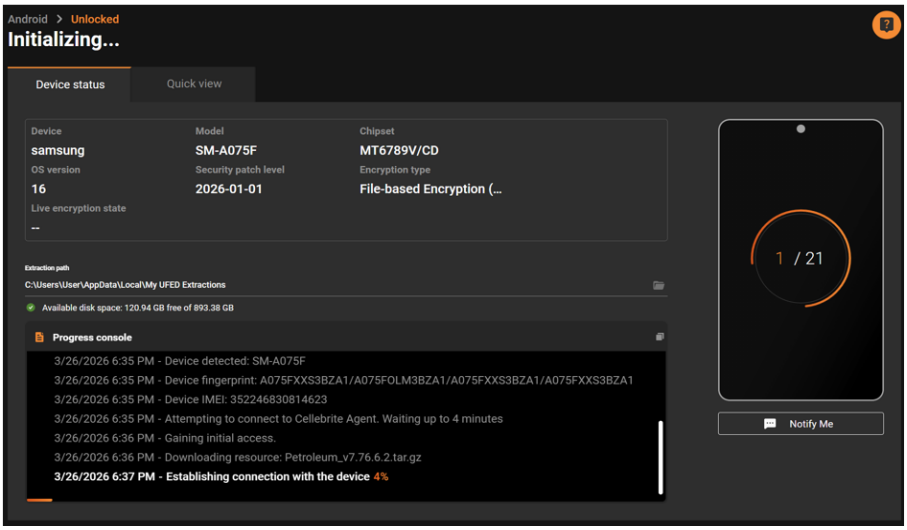


Figure 7. Initialization process
source: research data

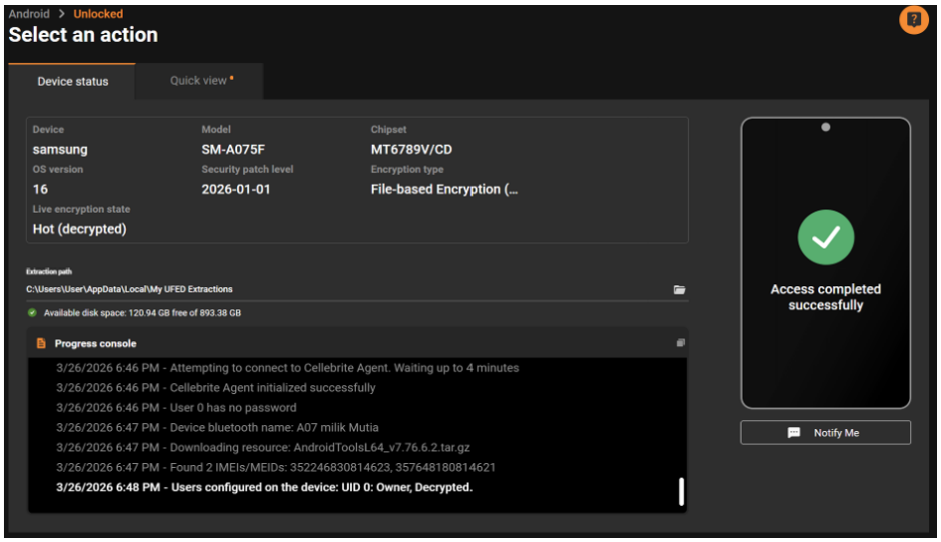


Figure 8. Initialization process completed
source: research data

Figures 7 and 8 show the completed initialization process carried out using Cellebrite UFED. At this stage, 21 configurations were performed by Cellebrite UFED and the phone to install an agent and ultimately decrypt all data on the phone.

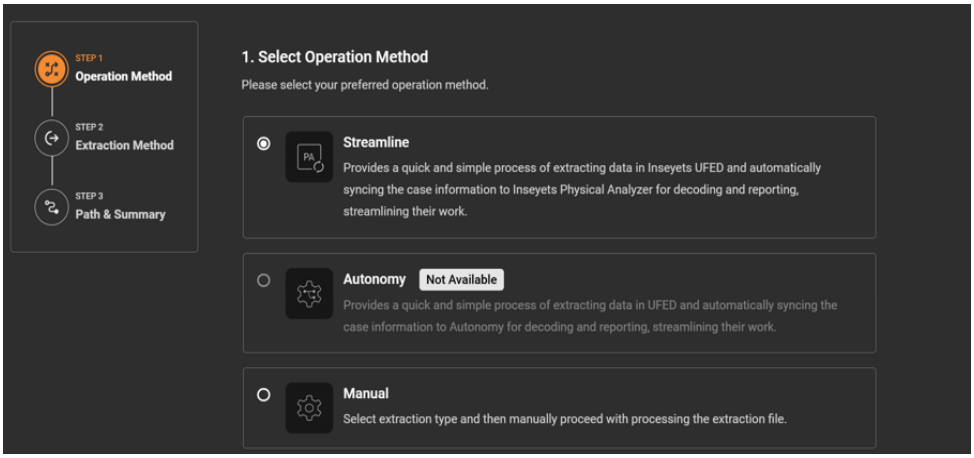


Figure 9. Operation Method
source: research data

Figure 9 shows three operation method options: Streamline, Autonomy, and Manual. This research used the Streamline feature, or streamline workflow, to simplify and accelerate the data extraction process from the phone because it does not require manual configuration and minimizes human error. The Autonomy feature could not be used at this time because of licensing limitations, whereas the Manual feature refers to a type of manual extraction that requires the operator to perform each step individually. After selecting the operation method, the next step is to choose the Extraction Method, Streamline Settings, and Path & Summary shown in Figure 10.

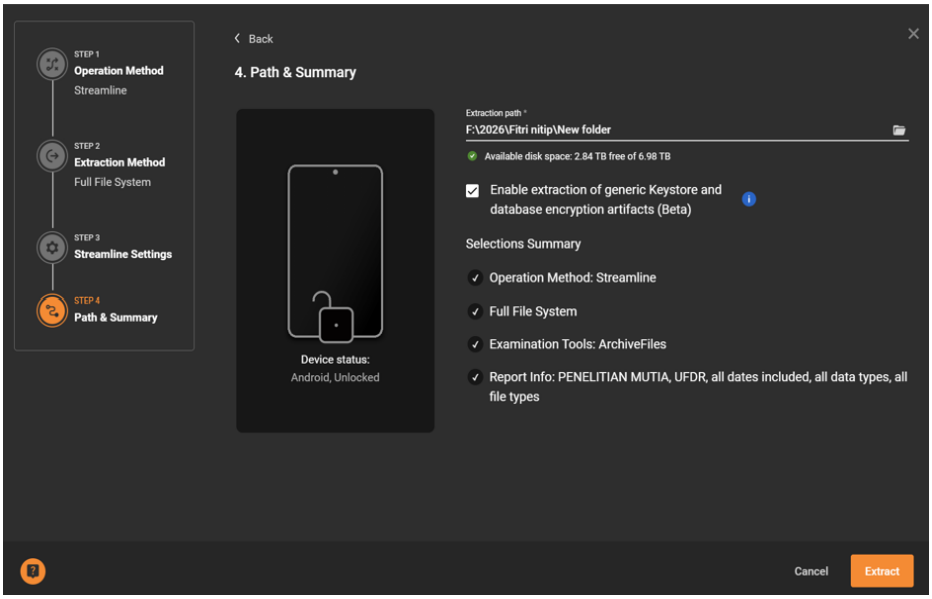


Figure 10. Path & Summary
source: research data

In the extraction method, there are six features that determine the extraction process. The researcher used the Full File System feature to ensure that all data from the active file system, including/ system/ location, could be extracted. Next, fill in the Streamline settings or case details to specify the file name and the file storage location.

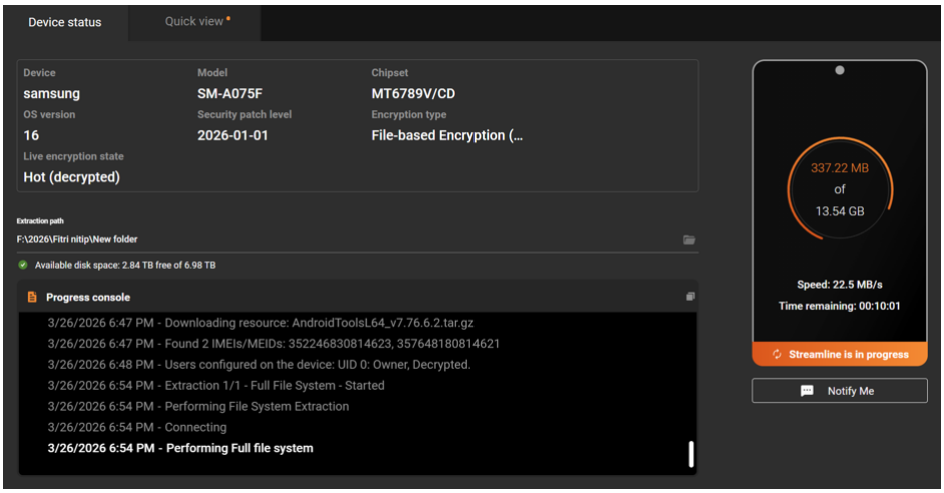


Figure 11. Performing Full File System
source: research data

Based on the display in Figure 11, it appears that data extraction was performed using the streamlined method on a Samsung SM-A075F device running the Android 16 operating system. The device is in a “Hot (decrypted)” state, indicating that it is powered on and unlocked, thereby allowing data stored within the file-based encryption (FBE) scheme to be accessed directly. Next, the system performs the Full File System extraction process, which provides a more comprehensive level of data acquisition than logical extraction. The extraction process is ongoing at a speed of approximately 22.5 MB/s, with an estimated total data volume of 13.54 GB, indicating that the streamlined method can automatically select the optimal extraction technique without requiring manual configuration by the examiner.

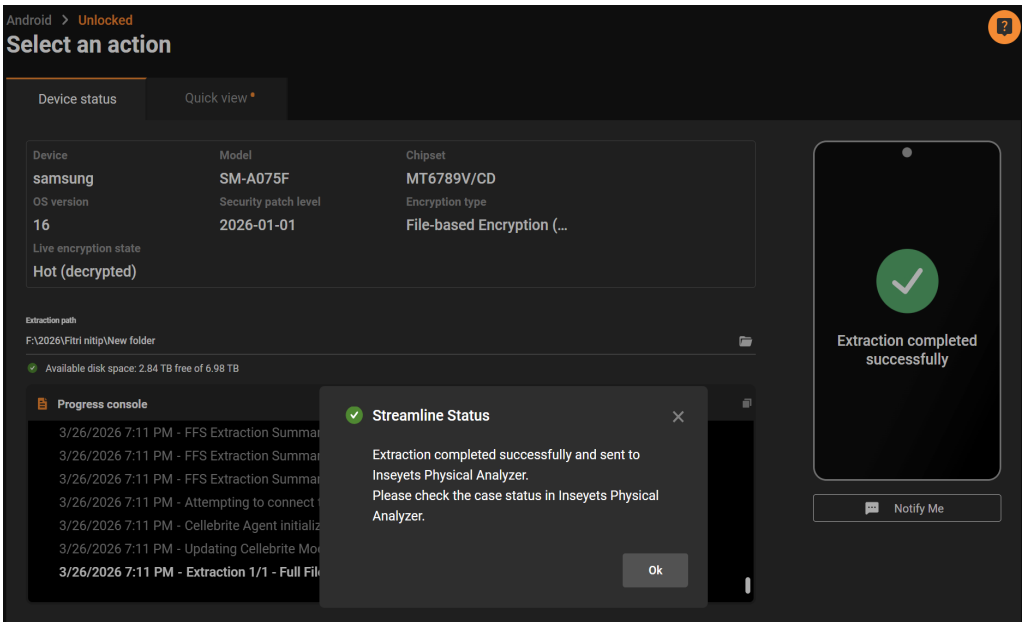


Figure 12. Extraction Completed Successfully
source: research data

Based on Figure 12, the extraction process was successfully completed, as indicated by the status, "Extraction Completed Successfully." This indicates that all extraction stages, including connection initialization, downloading supporting components, and executing the Full File System Extraction, were successfully carried out; subsequently, the extraction results could be analyzed using the analyzer application.

MD

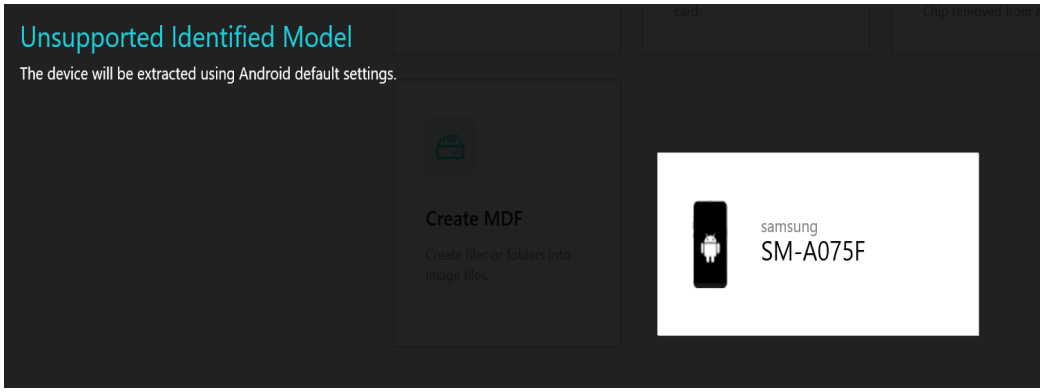


Figure 13. Extraction Method Selection Process
source: research data

Figure 13 explains that the phone used by the researcher does not support data extraction using the physical method because neither the device type nor the chipset of the Samsung Galaxy A07 Android phone is currently listed in the extractable device list on MD. Other methods that can be performed are shown in the figure 14.

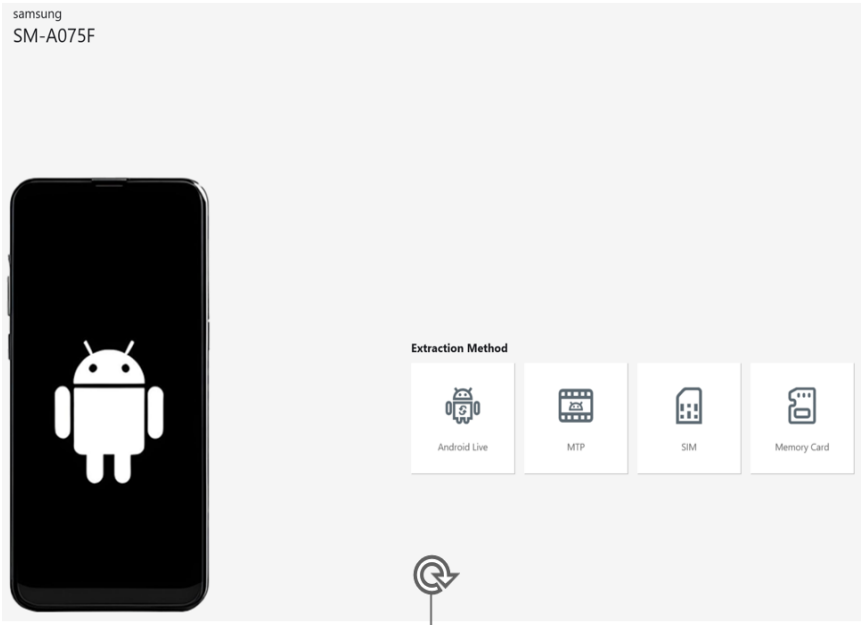


Figure 14. Extraction Method
source: research data

Figure 14 shows several available extraction method options: Android Live, MTP, SIM, and Memory Card. The researcher used the Android Live method to extract data directly from the Android operating system while the device was powered on and unlocked, allowing access to application and system data. After selecting the extraction method, the examiner entered the extraction information and selected the storage path for the extraction results shown figure 15.

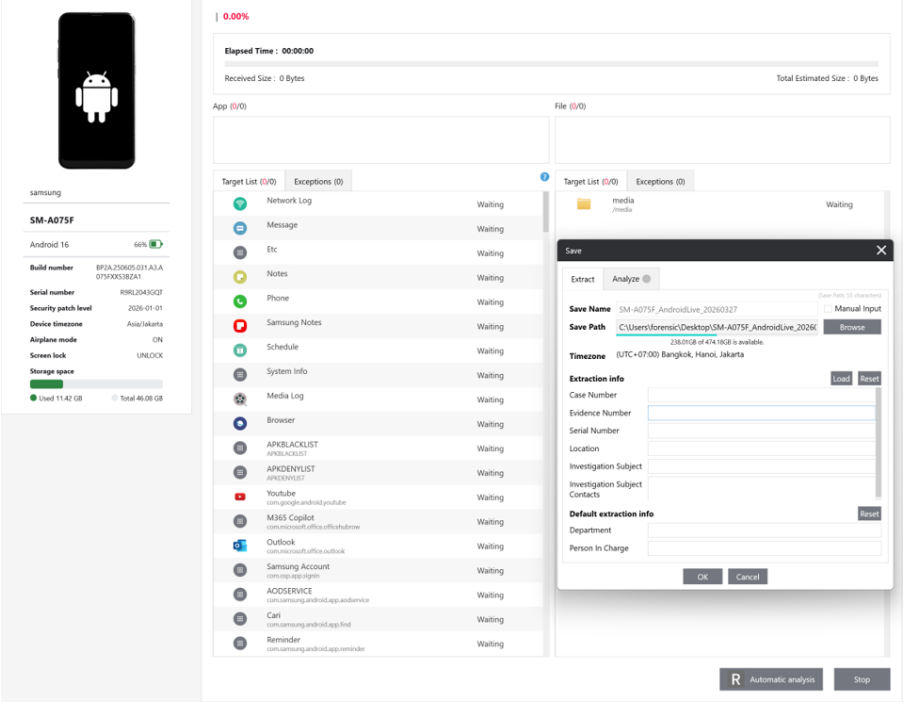


Figure 15. Extraction info, save path, dan progres
source: research data

The main part of the system displays a list of digital artifact targets, such as messages, phone records, media, browser data, system information, and various applications, with a "waiting" status indicating that the extraction process has not yet started. On the right side, a save configuration window appears, requiring action before the extraction process can begin. This display indicates that, prior to the extraction process, the examiner must ensure proper storage configuration to maintain the chain of custody and the integrity of the digital evidence.

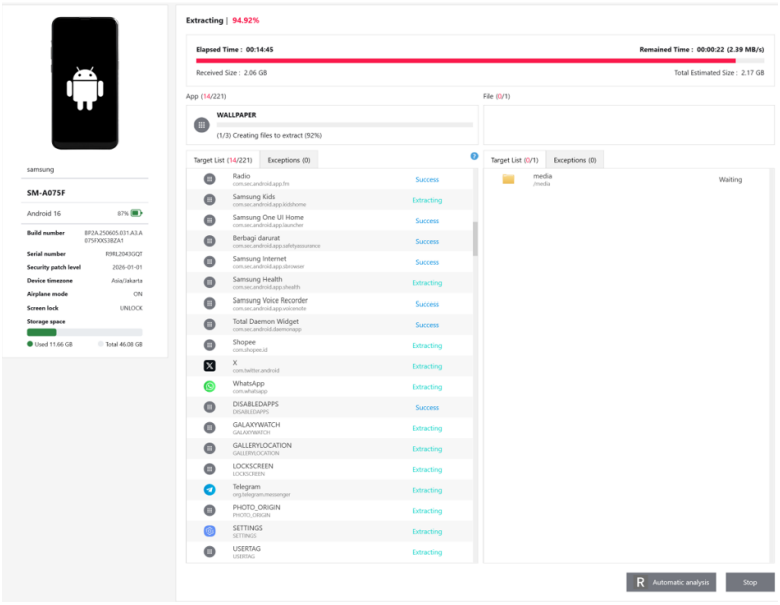


Figure 16. Dashboard
source: research data

This display shows the ongoing data extraction process, with progress reaching 94.92%. The main section displays a list of target artifacts and applications, such as WhatsApp, Telegram, and various system applications, with statuses ranging from Extracting to Success. This information indicates that the extraction method used can access various data sources from user applications. Subsequently, the extraction results will be analyzed using an application integrated with MD.

The next stage is examination. Previous research explained that the examination stage is used to ensure that the extracted data remains authentic and unaltered. In this study, after performing data acquisition on the mobile phone (imaging), the examination stage is conducted by the examiner for indexing purposes using software integrated with the extraction tool. This process enables further analysis by the examiner while maintaining the authenticity of the acquired data. Figures 17 and 18 are the data extraction results based on the created simulation.

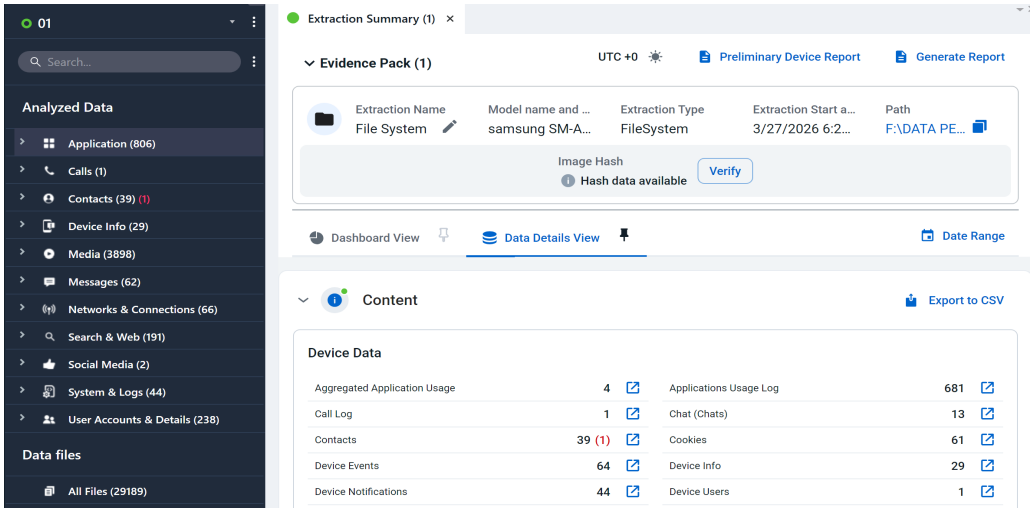


Figure 17. Ufed Cellebrite Extraction Results
source: research data

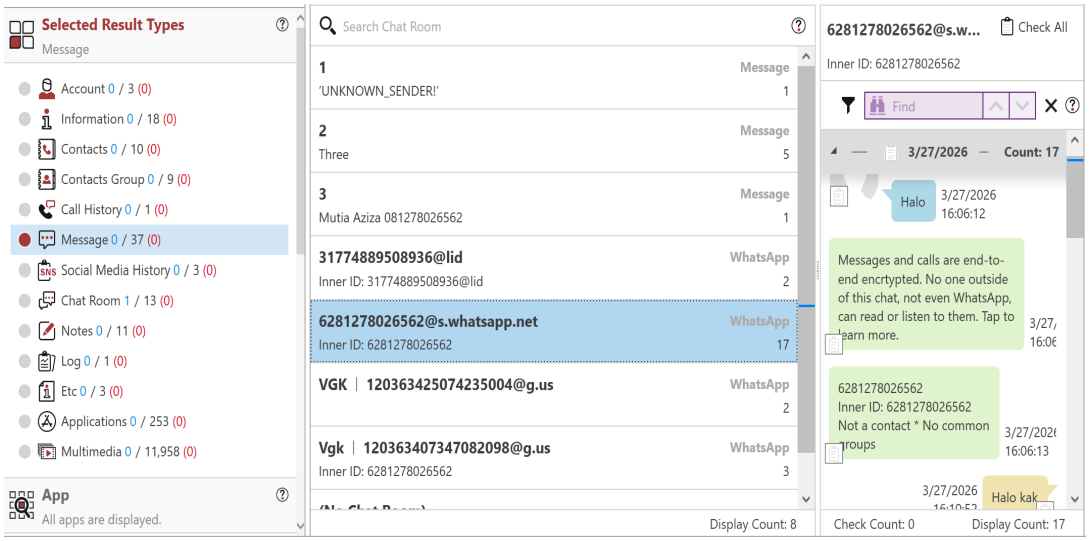
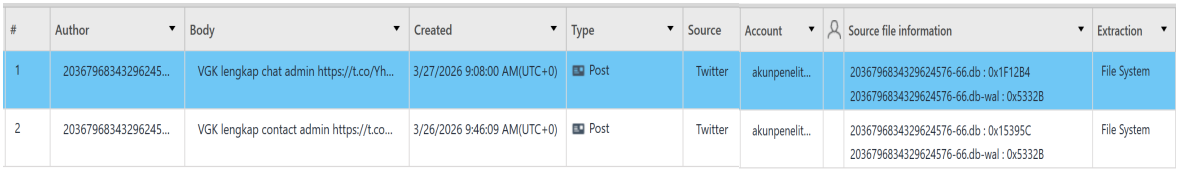


Figure 18. MD Extraction Results
source: research data

Figures 17 and 18 show extraction results obtained using UFED Cellebrite and MD, which were analyzed using forensic analysis software. From these figures, it can be seen that all forensic tools used were able to obtain artifacts through both Full File System and Android Live acquisition methods. This is evident from the extraction results, where various categories of digital artifacts, such as applications, messages, media, and others, are available.

The next stage is analysis. Previous research described the analysis process as involving the processing of examination results, reconstructing sequences of activities, and performing data recovery using specific forensic techniques to identify perpetrators, timing, and locations of manipulation incidents. In this study, the analysis stage is used to identify the data required based on the reported case by examining patterns, relationships, and relevant information. In this case, the researchers focus on data obtained from applications used in the crime simulation.

At this stage, the imaging or data acquisition results undergo indexing to convert raw data into a readable format using specialized forensic analysis software. The indexing results are then used for activity reconstruction to compile a chronological sequence of events. Figure 19 presents the indexing data.



#	Author	Body	Created	Type	Source	Account	Source file information	Extraction
1	20367968343296245...	VGK lengkap chat admin https://t.co/Yh...	3/27/2026 9:08:00 AM(UTC+0)	Post	Twitter	akunpenelit...	20367968343296245 76-66.db : 0x1F12B4 20367968343296245 76-66.db-wal : 0x5332B	File System
2	20367968343296245...	VGK lengkap contact admin https://t.co...	3/26/2026 9:46:09 AM(UTC+0)	Post	Twitter	akunpenelit...	20367968343296245 76-66.db : 0x15395C 20367968343296245 76-66.db-wal : 0x5332B	File System

Figure 19. Twitter application indexing Ufed Cellebrite
source: research data

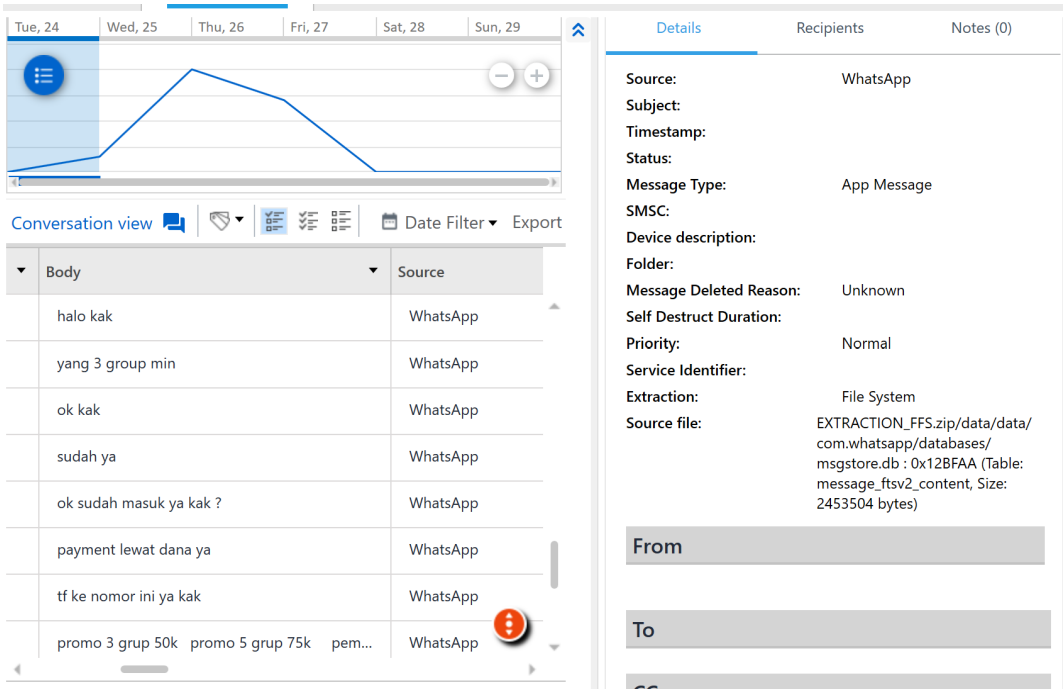


Figure 20. WhatsApp indexing results on Ufed Cellebrite
source: research data

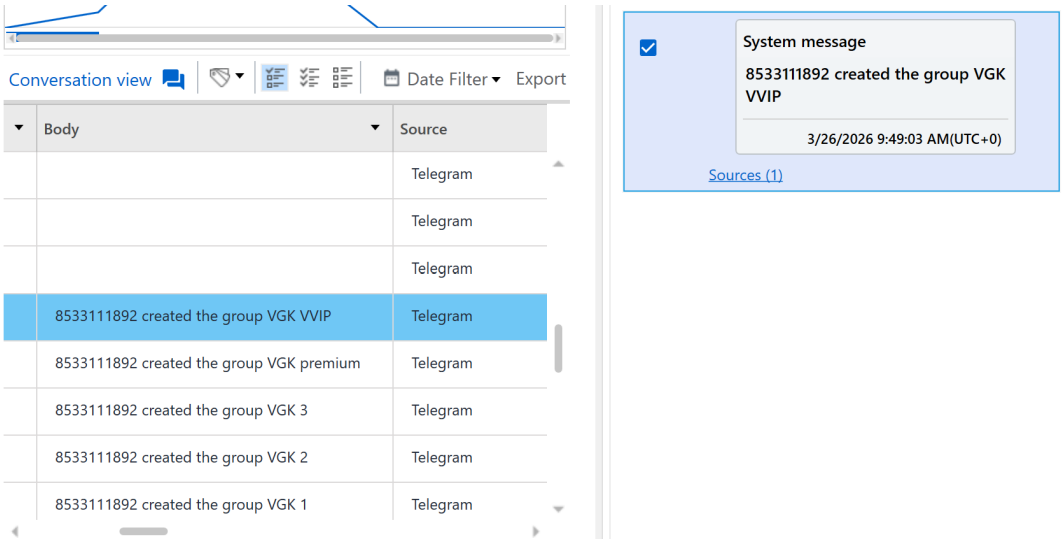
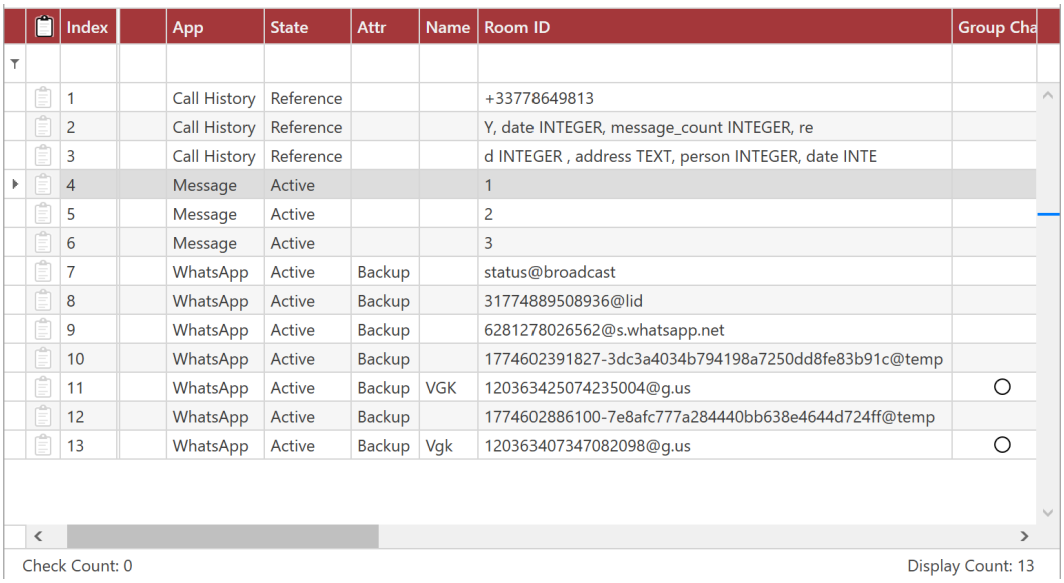


Figure 21. Telegram Indexing Results on MD
source: research data



Index	App	State	Attr	Name	Room ID	Group Cha
1	Call History	Reference			+33778649813	
2	Call History	Reference			Y, date INTEGER, message_count INTEGER, re	
3	Call History	Reference			d INTEGER , address TEXT, person INTEGER, date INTE	
4	Message	Active			1	
5	Message	Active			2	
6	Message	Active			3	
7	WhatsApp	Active	Backup		status@broadcast	
8	WhatsApp	Active	Backup		31774889508936@lid	
9	WhatsApp	Active	Backup		6281278026562@s.whatsapp.net	
10	WhatsApp	Active	Backup		1774602391827-3dc3a4034b794198a7250dd8fe83b91c@temp	
11	WhatsApp	Active	Backup	VGK	120363425074235004@g.us	○
12	WhatsApp	Active	Backup		1774602886100-7e8afc777a284440bb638e4644d724ff@temp	
13	WhatsApp	Active	Backup	Vgk	120363407347082098@g.us	○

Check Count: 0 Display Count: 13

Figure 22. MD Chat Room Indexing Results
source: research data

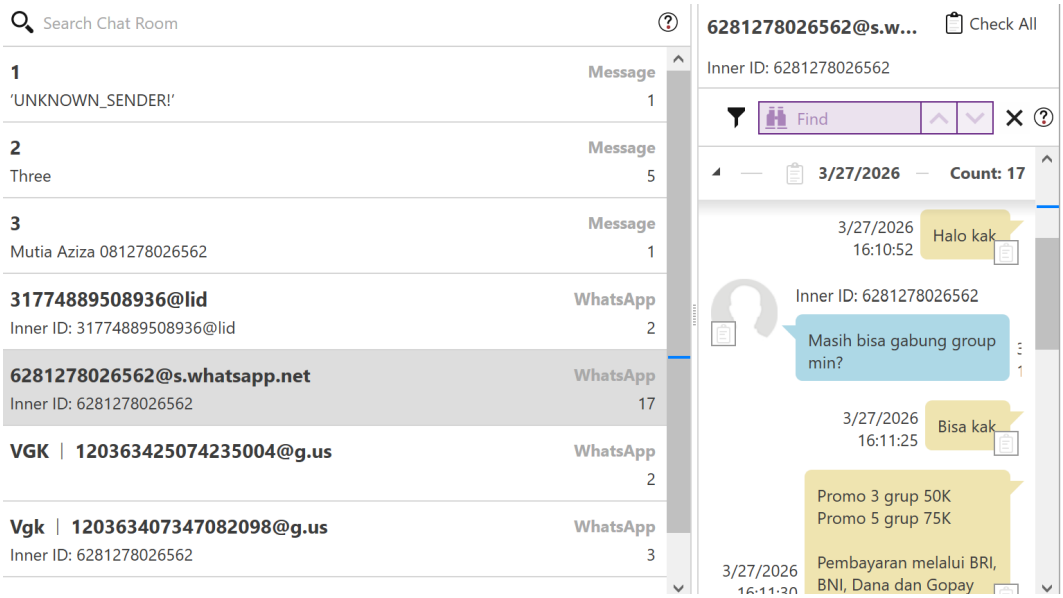


Figure 23. MD WhatsApp Indexing Results
source: research data

Figures 21 to 22 show that the Full File System acquisition method was able to obtain data more comprehensively, including all WhatsApp application conversations and activities, such as posting on the Twitter application. Meanwhile, the limitation in obtaining Telegram message data is due to the cloud-based storage architecture implemented; therefore, data is not fully stored on the device. Consequently, neither the Full File System nor Android Live methods could fully obtain Telegram message artifacts. However, in this research simulation, some Telegram activity artifacts, such as information related to creating Telegram groups, were still successfully obtained. The Android Live acquisition method could not obtain posting activity data on the Twitter application because the main Twitter data, such as posts and timelines, is stored in the phone's cache, and acquisition using Android Live does not retrieve file system data.

Next is the reporting stage. Previous research stated that this stage is the process of documenting the entire investigation process. Additionally, previous research proposed the addition of two feedback mechanisms: examination feedback and analysis feedback, which function as means of knowledge reintegration and reevaluation when there is a need for reporting completeness based on new information from the investigator or analysis results from the

examiner. Based on interviews with the examiner, reporting feedback can be implemented but depends on the extraction method used. If new information is provided by the investigator, the examiner will first return to the analysis stage to determine whether the required data has been acquired. If the data is available, the examiner will perform reanalysis through the analysis feedback mechanism. However, if the new information has not been acquired because of limitations in the extraction method used, the examiner will return to the data acquisition stage through the data acquisition feedback mechanism. Subsequently, the report is submitted to the investigator in the form of an Official Report.

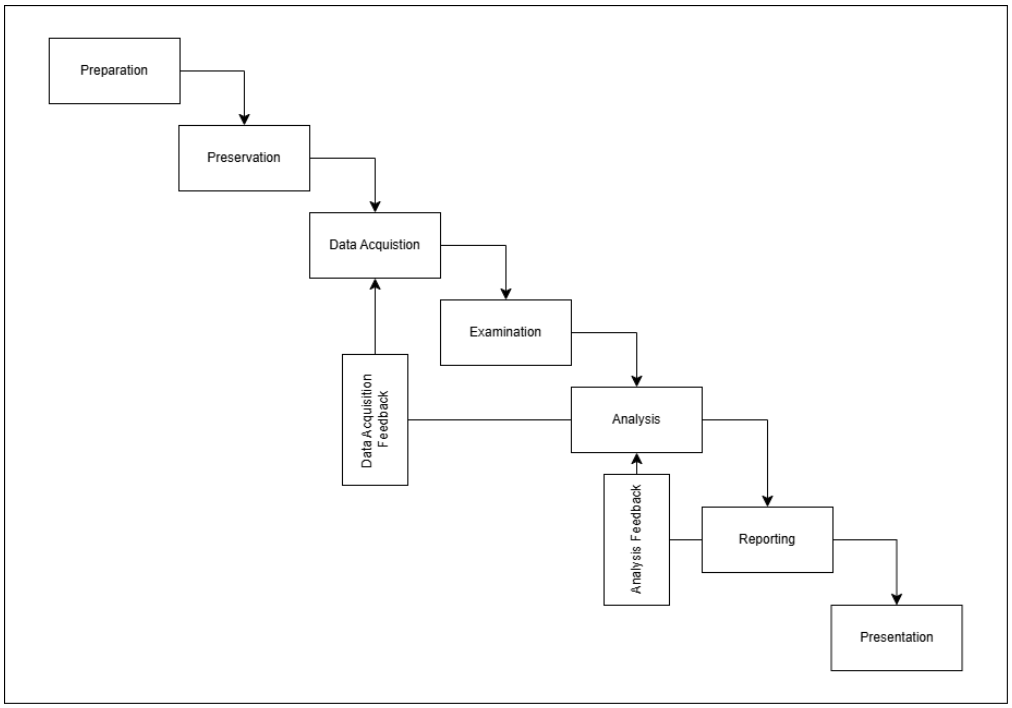


Figure 24. Proposed Improvement to the Feedback Mechanism in the HMFIPM Model
source: research data

Figure 24 presents a proposed improvement to the feedback mechanism in the HMFIPM model, focusing on the data analysis and data acquisition stages. This improvement aims to increase the effectiveness and flexibility of the digital forensic investigation process in responding to the dynamics of field findings during the reporting stage. Through analysis feedback, the examiner can reevaluate and reanalyze data that has been obtained if additional requirements or indications of discrepancies are identified. However, if the additional data required are not identified during the analysis stage, the examiner can use the acquisition feedback mechanism to acquire additional data that were previously not acquired due to limitations in the extraction method used.

Discussion

The results of this study indicate that the Harmonized Mobile Forensic Investigation Process Model (HMFIPM) can be systematically applied within a Digital Forensics Laboratory environment that adheres to the ISO/IEC 17025 standard. This applicability is evident from the sequential execution of the preparation, preservation, data acquisition, examination, analysis, reporting, and presentation stages in an investigation simulation involving an Android device. This finding aligns with the argument of Al-Dhaqm et al. (2021) that the development of digital forensics subdomains requires a harmonized process framework to ensure that investigations are consistent, documented, and accountable (Haluszka & Mansour, 2023). In the context of this research, HMFIPM not only functions as a conceptual model but also serves as an operational guideline that helps examiners maintain the integrity of digital evidence from the initial receipt of evidence to the presentation of examination results.

In the preservation and data acquisition stages, this research demonstrates that the

success of the extraction process is highly influenced by the compatibility among the device, extraction method, and tools used. The use of Cellebrite UFED with the Full File System extraction method produced more complete artifacts compared to MD, which in this case could only use the Android Live extraction method. These results align with Parhad and Naik (2023), who emphasized that the effectiveness of data extraction on Android devices highly depends on chipset support, device model, and acquisition method compatibility. This finding also supports the view of El Majdoub et al. (2022) that the mobile forensics acquisition process cannot be fully standardized because each device has different technical characteristics; therefore, the selection of extraction techniques must be adapted to the device condition and investigation objectives.

In the examination and analysis stages, the research results show that the extracted data can be parsed and indexed to produce relevant artifacts such as messages, application logs, metadata, and user activities. However, the ability to obtain certain artifacts remains limited by the application's storage architecture. In this study, WhatsApp artifacts could be obtained more completely, whereas Telegram artifacts were not fully recovered because most of their data are cloud-based. This finding aligns with the study by Mahajan et al. (2013), which showed that each instant messaging application has a different artifact storage pattern; therefore, the results of forensic examinations are highly influenced by the application's design (Shetty & Trevorrow, 2026; Son et al., 2022). This result is also supported by Millatina et al. (2024), who explained that applications such as WhatsApp, Instagram, and Telegram on Android devices yield different levels of artifact recoverability, thus requiring investigators to understand the technical characteristics of each application before drawing forensic conclusions (Femi-Adeyinka et al., 2024; Knox et al., 2020; Sinaga et al., 2026).

This research also confirms that the quality of investigation results is not solely determined by the HMFIPM model but rather by the combination of the process model, tool capabilities, and the validity of laboratory working procedures. In this regard, HMFIPM is better understood as an investigation framework that organizes the workflow, whereas the artifact extraction results are highly dependent on the technical performance of the forensic software. This view aligns with Cuomo et al. (2022), who highlighted that technical assessments in mobile forensics can be repeatable or nonrepeatable, depending on the device condition, tool, and examination procedures. This means that even if the investigation model is well structured, examination results may differ if the technical environment and extraction methods change.

Another important aspect resulting from this research is the evaluation of the feedback mechanism in HMFIPM. Theoretically, examination feedback and analysis feedback are designed to allow examiners to return to previous stages when data deficiencies or new analytical requirements are identified. However, the research results show that this mechanism is not yet fully adequate for the dynamics of real investigations. In laboratory practice, when the need for additional artifacts that were not acquired is identified, the examiner cannot merely return to the analysis stage but must also consider returning to the acquisition stage. This finding relates to the importance of chain of custody and digital evidence governance that are flexible yet secure, as discussed by Nath et al. (2024) and Singh et al. (2022), who argued that modern digital evidence management requires adaptive procedures without compromising evidence integrity and accountability.

Overall, this research reinforces that HMFIPM is worthy of consideration as a standardized mobile forensic investigation process model, particularly because it provides a clear workflow structure for examining Android devices. However, this feasibility still requires refinement, especially in the feedback mechanism, to better accommodate actual investigation needs in the laboratory (Jawad et al., 2020; Riadi et al., 2023; Sutikno, 2024). Thus, the main contribution of this research lies not only in the empirical validation of the HMFIPM model in Indonesia but also in proposing practical improvements to make the model more responsive to technical extraction limitations and the dynamics of forensic findings in the field (Agustiono et al., 2024; Al-Dhaqm et al., 2021; Sharma et al., 2022).

CONCLUSION

The validation of the Harmonized Mobile Forensic Investigation Process Model (HMFIPM) conducted in an ISO/IEC 17025-accredited forensic laboratory demonstrates that the model is feasible as a standardized framework for mobile forensic investigations. The implementation of HMFIPM provided a structured workflow for conducting mobile forensic investigations, particularly through the stages of preparation, preservation, data acquisition, examination, analysis, and reporting.

However, the findings indicate that the feedback mechanisms in HMFIPM still require further refinement to make the model more adaptive to real-world investigative dynamics. Although HMFIPM provides a systematic process framework, the completeness of the acquired digital artifacts may still be affected by technical factors such as forensic tool capability, device compatibility, and the selected extraction method. Therefore, the model should explicitly accommodate feedback from the examination or analysis stages back to the data acquisition stage when additional artifacts are required or when the initial extraction method is unable to obtain relevant evidence.

Accordingly, this study proposes a refinement of the HMFIPM feedback mechanism by emphasizing not only analysis feedback but also data acquisition feedback. This refinement is expected to improve the applicability of HMFIPM in forensic laboratory practice, particularly in handling variations in extraction results, tool limitations, and the dynamic nature of mobile forensic investigations.

ACKNOWLEDGEMENT

The authors gratefully acknowledge the Digital Forensics Laboratory, accredited under ISO/IEC 17025, for providing access to forensic tools and for the time of the examiners and investigators who participated in the qualitative interviews. The authors also thank Universitas Indonesia for institutional support and the anonymous reviewers whose constructive feedback substantially improved this manuscript.

AUTHOR CONTRIBUTION STATEMENT

Author 1: conceptualization, methodology, data acquisition, formal analysis, writing - original draft. Author 2: supervision, validation, methodology review, writing - review and editing. Both authors have read and approved the final manuscript.

REFERENCES

Agustiono, W., Suci, D. W., & Prastiti, N. (2024). Analisis Forensik Digital Menggunakan Metode NIST untuk Memulihkan Barang Bukti yang Dihapus. *Jurnal Teknologi Dan Informasi*, *14*(2), 174–185. https://doi.org/10.34010/jati.v14i2.12952

Al-Dhaqm, A., Ikuesan, R. A., Kebande, V. R., Razak, S. A., Grispos, G., Choo, K.-K. R., Al-Rimy, B. A. S., & Alsewari, A. A. (2021). Digital Forensics Subdomains: The State of the Art and Future Directions. *IEEE Access*, *9*, 152476–152502. https://doi.org/10.1109/ACCESS.2021.3124262

Banesinh, V. J. (2025). *Detection of Cyber Crimes via Digital Forensic Artifacts*. Gujarat Technological University.

Cuomo, R., D'Agostino, D., & Ianulardo, M. (2022). Mobile Forensics: Repeatable and Non-Repeatable Technical Assessments. *Sensors*, *22*(18), 7096. https://doi.org/10.3390/s22187096

El Majdoub, A., Saadi, C., & Chaoui, H. (2022). Mobile Forensics Data Acquisition. *ITM Web of Conferences*, *46*, 02006. https://doi.org/10.1051/itmconf/20224602006

Femi-Adeyinka, C., Kose, N. A., Akinsowon, T., & Varol, C. (2024). Digital Forensics Analysis of YouTube, Instagram, and TikTok on Android Devices: A Comparative Study. *2024 12th International Symposium on Digital Forensics and Security (ISDFS)*, 1–6. https://doi.org/10.1109/ISDFS60797.2024.10527244

Fukami, A., Stoykova, R., & Geradts, Z. (2021). A new model for forensic data extraction from encrypted mobile devices. *Forensic Science International: Digital Investigation*, *38*, 301169.

Haluszka, E., & Mansour, A. (2023). *A comparative review of ISO standards for digital forensics*

laboratory accreditation.

Hamad, N., & Eleyan, D. (2022). Digital forensics tools used in cybercrime investigation-comparative analysis. *Journal of Xi'an University of Architecture & Technology*, *4*, 113–127.

Jawad, M., Nadeem, M. S. A., Shim, S.-O., Khan, I. R., Shaheen, A., Habib, N., Hussain, L., & Aziz, W. (2020). Machine Learning Based Cost Effective Electricity Load Forecasting Model Using Correlated Meteorological Parameters. *IEEE Access*, *8*, 146847–146864. https://doi.org/10.1109/ACCESS.2020.3014086

Knox, S., Moghadam, S., Patrick, K., Phan, A., & Choo, K.-K. R. (2020). What's really 'Happning'? A forensic analysis of Android and iOS Happn dating apps. *Computers & Security*, *94*, 101833. https://doi.org/10.1016/j.cose.2020.101833

Mahajan, A., S. Dahiya, M., & P. Sanghvi, H. (2013). Forensic Analysis of Instant Messenger Applications on Android Devices. *International Journal of Computer Applications*, *68*(8), 38–44. https://doi.org/10.5120/11602-6965

Millatina, D., Gunawan, E. H., & Sugiantoro, B. (2024). Forensic Analysis of WhatsApp, Instagram, and Telegram on Virtual Android Device. *2024 12th International Symposium on Digital Forensics and Security (ISDFS)*, 1–4. https://doi.org/10.1109/ISDFS60797.2024.10527308

Nath, S., Summers, K., Baek, J., & Ahn, G.-J. (2024). Digital Evidence Chain of Custody: Navigating New Realities of Digital Forensics. *2024 IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA)*, 11–20. https://doi.org/10.1109/TPS-ISA62245.2024.00012

Parhad, O., & Naik, V. (2023). Comparative analysis of Data Extraction for Qualcomm based android devices. *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, 1–7. https://doi.org/10.1109/ICCCNT56998.2023.10307241

Riadi, I., Yudhana, A., Pramuja, G., & Fanani, I. (2023). Mobile Forensic Tools for Digital Crime Investigation: Comparison and Evaluation. *International Journal of Safety and Security Engineering*, *13*(1), 11–19. https://doi.org/10.18280/ijsse.130102

Şen, S., & Artuner, H. (2025). Emulator Forensics Investigation Model (EFIM). *IEEE Access*.

Sharma, Y. K., Noval, S. S., Jain, A., Sabitha, B., & Ramya, T. (2022). Forensics-as-a-service: A Review of Mobile Forensics. *2022 5th International Conference on Contemporary Computing and Informatics (IC3I)*, 486–491. https://doi.org/10.1109/IC3I56241.2022.10072726

Shetty, A. A., & Trevorrow, P. (2026). Digital Forensic Investigation of Wearable Android Fitness Applications. *Journal of Applied Security Research*, *21*(1), 35–59. https://doi.org/10.1080/19361610.2025.2562398

Sinaga, S. J., Asykar, M. A., Manurung, H., Wibowo, W. C., Yazid, S., & Edwardo, T. O. (2026). Comparative evaluation of artifact extraction performance and usability in digital forensic tools: A study of Cellebrite UFED, MSAB XRY, and Magnet AXIOM. *Journal of Forensic Sciences*. https://doi.org/10.1111/1556-4029.70320

Singh, A., Ikuesan, R. A., & Venter, H. (2022). Secure Storage Model for Digital Forensic Readiness. *IEEE Access*, *10*, 19469–19480. https://doi.org/10.1109/ACCESS.2022.3151403

Son, J., Kim, Y. W., Oh, D. Bin, & Kim, K. (2022). Forensic analysis of instant messengers: Decrypt Signal, Wickr, and Threema. *Forensic Science International: Digital Investigation*, *40*. https://doi.org/10.1016/j.fsidi.2022.301347

Sutikno, T. (2024). Mobile forensics tools and techniques for digital crime investigation: a comprehensive review. *International Journal of Informatics and Communication Technology (IJ-ICT)*, *13*(2), 321–332.