

Digital Forensic Analysis of a Case of Pornographic Content Dissemination on WhatsApp Using the National Institute of Standards and Technology (NIST) Method

A.Abdi Fahrul Islam^{a,1}, Muh Ichlasul Amal Syam^{a,2}, Ramdan Satra^{a,3}, Erick Irawadi Alwi^{a,4}

^a Informatics Engineering Study Program, Faculty of Computer Science, Universitas Muslim Indonesia, Jl. Urip Sumoharjo KM.05, Makassar 90231, Indonesia

¹ andiabdi2003@gmail.com; ² muhichlasulamalsyam@gmail.com; ³ ramdan@umi.ac.id; ⁴ erick.alwi@umi.ac.id

ARTICLE INFORMATION	ABSTRACT
Received : 22 – 08 – 2026 Revised : 24 – 09 – 2026 Published : 05 – 11 – 2026	The dissemination of pornographic content through instant messaging applications such as WhatsApp is becoming increasingly widespread. A major obstacle to establishing legal proof in these cases is that perpetrators frequently use the "Delete for Everyone" feature to eliminate digital evidence. This study aims to apply the National Institute of Standards and Technology (NIST) method to obtain digital artifacts from messages deleted on the perpetrator's device. A simulated scenario was conducted between the victim's device (Xiaomi Redmi 10C) and the perpetrator's device (a rooted Xiaomi Redmi S2). The investigation used MOBILedit Forensic Express for physical acquisition and Belkasoft Evidence Center for data analysis. The results show that the NIST framework successfully overcame anti-forensic obstacles. The recovered digital evidence included metadata from 3 deleted text messages with logical deletion status, 3 image files containing pornographic content (.tmp/.jpeg), and 2 video files (.mp4). Cross-validation between fragments from the perpetrator's msgstore.db database and the victim's screenshots demonstrates that this method can produce legally valid and compelling electronic evidence for court proceedings.
Keywords: Digital Forensics WhatsApp Pornography NIST Method Artifacts	

I. Introduction

The rapid development of information and communication technology has become an integral part of modern society [1]. Increasingly easy access to various instant messaging applications has driven a substantial increase in the use of multimedia features for communication and data exchange [2]. In Indonesia, WhatsApp unequivocally dominates digital communication. This is confirmed by the 2025 report from We Are Social and Meltwater, which ranks WhatsApp as the leading social media platform, with a usage rate of 90.8% among the country's 180 million active social media users [3].

However, behind the convenience and extensive reach offered by this platform lies a darker side, in which its advanced features are also misused to facilitate cybercrime, particularly the dissemination of pornographic content. The importance of addressing this issue seriously is reinforced by official data from the Ministry of Communication and Informatics (Kominfo) of the Republic of Indonesia, which recorded the handling of 233,552 items of pornographic content within a short period [4]. The situation becomes even more concerning when considering data from the National Criminal Information Center (Pusiknas) of the Indonesian National Police Criminal Investigation Agency as of November 2025, which recorded 596 reported pornography cases. This figure represents an increase of 17.55% compared with the same period in the previous year, with most transmission and dissemination associated with these sexual offenses occurring through social media and instant messaging applications [5].

A major difficulty frequently encountered by police and investigators when handling pornography cases on WhatsApp is perpetrators' use of the "Delete for Everyone" feature. This feature allows users to retract or delete messages that have already been sent from both the sender's and the recipient's devices. In criminal investigations, this feature is often used as an anti-forensic measure to eliminate digital traces and instantly destroy evidence. This situation calls for digital forensic research that not only focuses on data recovery techniques but also guarantees the integrity and validity of the recovered evidence so that it is legally valid and admissible in court.

Previous studies have focused on forensic analysis of social media and instant messaging applications to address these challenges. Research by Supardin et al. demonstrated the effectiveness of the National Institute of Standards and Technology (NIST) framework by comparing Magnet AXIOM and MOBILedit Forensic Express on Instagram Messenger, showing that these tools could recover deleted data with adequate accuracy [6]. In a different context, Karseno and Hendrik investigated the recovery of deleted WhatsApp messages using the National Institute of Justice (NIJ) method. They concluded that, although users had deleted the messages through the interface, the system merely marked their digital artifacts as "deleted" (logical deletion), while the physical data remained in memory and could be recovered [7].

Furthermore, Raharja et al. applied forensic methods to an online prostitution case on WhatsApp, successfully acquiring conversation and image artifacts from an Android device as legally valid evidence [8]. Meanwhile, Nasirudin et al. demonstrated the effectiveness of combining the NIST standard with MOBILedit in preserving the authenticity and integrity of data on Android devices [9]. Similarly, Rifqi et al. applied NIST SP 800-86 to WhatsApp analysis using FTK Imager and SQLite Browser, demonstrating a systematic approach that procedurally preserved digital evidence integrity [10]. The validity of digital evidence obtained through standardized methods was also demonstrated by Kusuma et al. for physical storage media [11] and by Hidayat et al. for video evidence from social media platforms [12].

Although these studies have comprehensively addressed forensic aspects of social media, most research still focuses on standard extraction without specifically emphasizing evidentiary validation when message text cannot be fully reconstructed because of encryption and advanced data wiping. No study has specifically integrated the NIST method with cross-validation techniques (cross-synchronization) to address cases of pornographic content dissemination on WhatsApp affected by deliberate message deletion.

Based on this research gap, this study aims to implement and describe in detail the application of each stage of the NIST method, from Collection and Examination to Analysis and Reporting, in a digital forensic investigation. The study focuses on identifying, extracting, and analyzing hidden digital artifacts, such as deleted text message metadata, cached pornographic images, and obscene video files, to produce valid electronic evidence that conclusively supports the legal substantiation of criminal offenses.

II. Methods

A. Forensic Stages of the NIST Method

The digital forensic investigation of the perpetrator's device was conducted in accordance with the international standard guidelines of the National Institute of Standards and Technology (NIST) Special Publication 800-86, formulated by Kent et al. [13], as shown in Figure 2.

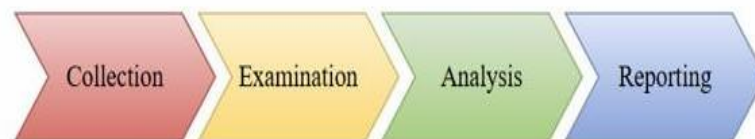


Figure 1. Stages of the NIST Forensic Framework

As shown in Figure 2, this method consists of four main stages carried out sequentially:

1. **Collection:** This stage focuses on identifying and securing physical evidence, namely the smartphone used in the case scenario. Initial device documentation, including its powered-on state and identifying details, is performed at this stage. Preservation measures are also implemented by isolating the device from networks using Airplane Mode to prevent data contamination from automatic synchronization, incoming notifications, or possible remote wipe commands [14].
2. **Examination:** This stage involves acquiring and extracting digital artifacts from the device to the examiner's computer. In this study, MOBILedit Forensic Express was used as the primary tool for copying and extracting WhatsApp artifacts from the Android device. The examination output included the WhatsApp application folder structure, database files such as msgstore.db and supporting files where available, and an extraction report (Report.pdf) listing multimedia artifacts, including images and videos, together with their file metadata. The objective of this stage is to obtain acquired data that can be analyzed without modifying the source data being examined [15].
3. **Analysis:** This stage focuses on the technical evaluation of the WhatsApp artifacts obtained in the preceding stage. The main analysis was conducted on the msgstore.db message database to identify conversation

artifacts and message metadata. Because low-level examination of msgstore.db displayed only unstructured text fragments, this study used Belkasoft Evidence Center (Trial) to parse the WhatsApp database so that message artifacts could be displayed together with forensic metadata, including timestamps, message direction (Outgoing), delivery status (Sent), and deletion status (Is Deleted). Multimedia analysis was also performed using the Report.pdf generated by MOBILedit to identify WhatsApp image and video artifacts and their file metadata, including names, paths, sizes, durations/dimensions, and Modified/Accessed times. Cross-validation was also performed among the victim's screenshots, keyword fragments from msgstore.db, and timestamps in the Belkasoft metadata to strengthen chronological reconstruction.

4. *Reporting*: This stage presents all findings in a structured and transparent manner to support the accountability of the investigation results. The report includes a summary of the identified artifacts, comprising deleted message metadata and image and video artifacts; a table matching the victim's evidence with the forensic findings; and conclusions addressing the research problem. The presentation emphasizes verifiable evidence, including message metadata (Outgoing, Sent, Is Deleted, and timestamps) and multimedia file metadata obtained from the extraction, so that the findings can be understood and used as a basis for forensic reporting in accordance with evidentiary requirements.

B. Research Design and Scenario

This study was designed around a simulated criminal scenario involving the dissemination of obscene content that represents real incidents in society. The simulation was necessary to create a valid condition of "evidence loss" for recovery testing. The scenario involved two parties: a female victim identified by the initials AN and a male perpetrator identified by the initials RD.

The scenario began on February 26, 2026, at approximately 12:15 WITA (Central Indonesia Time), when the victim (AN) received private WhatsApp messages from an unfamiliar number. The messages were sent by the perpetrator (RD) and consisted of 3 harassing text messages, 3 obscene image files, and 2 video files containing pornographic content. The victim had opened the messages. Recognizing the digital harassment, AN immediately took a precautionary step by capturing a screenshot of the chat.

At approximately 12:24 WITA, RD carried out an anti-forensic action by deleting all the messages he had sent using "Delete for Everyone" to eliminate traces of the crime from both devices. The following day, AN reported the incident to the police, presenting the screenshot as preliminary evidence. Investigators successfully established RD's identity, and at 18:15 WITA the police, simulated by the researchers, seized the perpetrator's smartphone while it was still powered on, as shown in Figure 1.

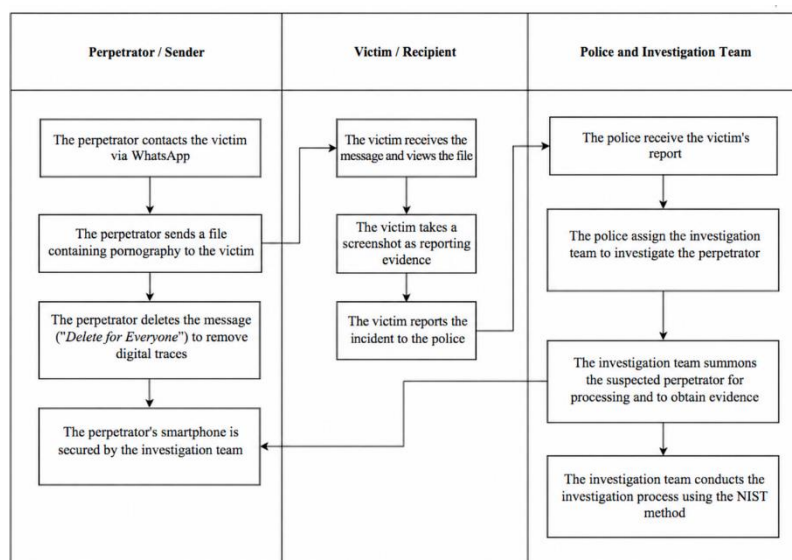


Figure 2. Research Workflow and Case Investigation Scenario

III. Results and Discussion

This section presents the results of applying the NIST framework to the established case scenario, followed by an in-depth discussion of the validity of the findings.

A. Collection

The Collection stage focused on securing the evidence to ensure that the data on the smartphone underwent no modification whatsoever after it was seized from the perpetrator. When investigators secured the perpetrator's smartphone (Xiaomi Redmi S2) at 18:15 WITA, the device was powered on. The investigators first visually documented the device's physical appearance and recorded its IMEI number (869146028937457), specifications (4 GB RAM, 64 GB ROM, and Android 9), and last displayed screen.

The most crucial preservation measure was promptly performed at 18:20 WITA by enabling Airplane Mode. This action disconnected all wireless connectivity on the device, including Wi-Fi, Bluetooth, and cellular data. This isolation was essential to prevent a potential remote wipe by the perpetrator's associates or incoming messages that could overwrite the storage memory containing deleted artifacts.

Next, to allow the forensic software to access the device's memory layer, the investigators opened Settings, tapped Build Number seven times to reveal Developer Options, and enabled USB Debugging. This configuration provided a system-level communication bridge between the perpetrator's Android device and the forensic workstation.

B. Examination

During the Examination stage, the perpetrator's smartphone was connected to the computer using a high-quality USB Type-C data cable to prevent transfer disruptions. Acquisition was performed using MOBILedit Forensic Express.

Because the operating system security access privileges on the perpetrator's Xiaomi Redmi S2 had been modified (Rooted/Superuser), MOBILedit automatically detected this status and offered the highest-level extraction option, Physical Extraction. This method is far superior to Logical Extraction because it can acquire an identical physical copy of the internal memory, or bit-by-bit image, including unallocated space and hidden application system files such as the WhatsApp cache folder and encrypted databases.

The acquisition process was completed, producing an image file and an extraction report without altering the original data structure on the perpetrator's device. This was demonstrated by verification of consistent cryptographic hash values between the data on the original device and the extracted data on the investigator's computer, as shown in Figure 3.

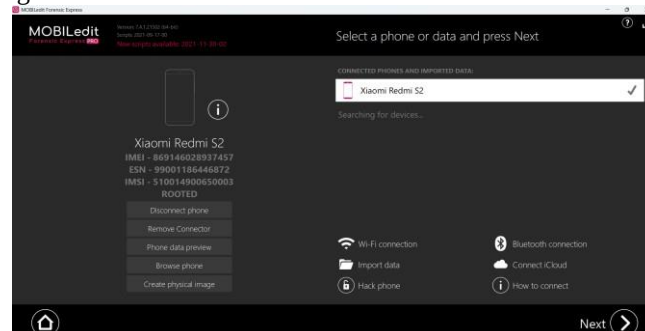


Figure 3. The Perpetrator's Smartphone Connected to MOBILedit Forensic Express

C. Analysis

The main focus of the Analysis stage was to trace artifacts within the extracted WhatsApp application directory, specifically the chat database (msgstore.db) and media storage directories for images and videos. Because the perpetrator had attempted an anti-forensic action using Delete for Everyone, manual low-level examination of msgstore.db with a conventional SQLite viewer displayed only fragmented, random text that had lost its relational metadata structure.

To resolve this issue, the image file was imported into and analyzed using Belkasoft Evidence Center X, which is equipped with deep parsing algorithms for encrypted messaging application databases.

Belkasoft's parsing successfully bypassed the deletion markers in the WhatsApp system. Three text message activity entries were identified from the perpetrator's number. Through the Properties menu, Belkasoft displayed crucial metadata. All three messages were validly recorded with the attributes Direction: Outgoing and Delivery Status: Sent, indicating successful delivery to the victim's device.

Furthermore, although WhatsApp had marked the messages so that they would not appear in the interface (logical deletion), Belkasoft extracted the attribute Is Deleted: Yes together with highly precise sending timestamps down to the second: 26/02/2026 at 12:15:40, 12:17:13, and 12:19:42. This finding confirms that the communication activity actually occurred, even though the text was hidden. The metadata evidence is presented in Figure 4.

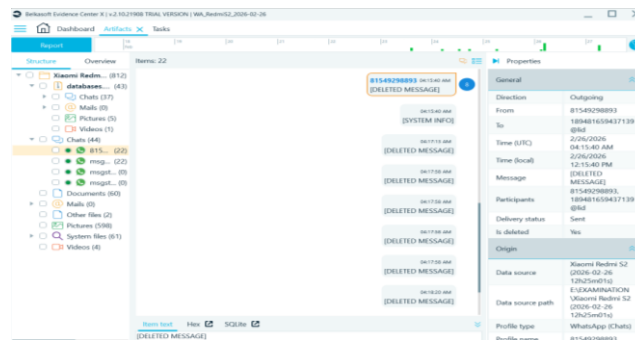


Figure 4. WhatsApp Message Metadata Displayed in Belkasoft

Cross-Synchronization Validation:

A common obstacle in deleted-message forensics is the loss of the original text content from the sender's database, which may raise doubts about "what the conversation actually contained." To address this limitation, this study introduces the application of a cross-device validation technique as its novelty.

The investigators retrieved random text fragments (low-level strings) remaining in the perpetrator's msgstore.db file, including occurrences of the keywords "syg", "kenalan", "cuek", "video", and "bareng". These isolated words were then matched against the complete screenshot of the chat history provided from AN's device. Synchronization was validated using timestamps extracted from Belkasoft metadata. The matching process was validated by comparing the visual evidence in Figure 5 and Figure 6, and the synchronization results were subsequently summarized in Table 1.

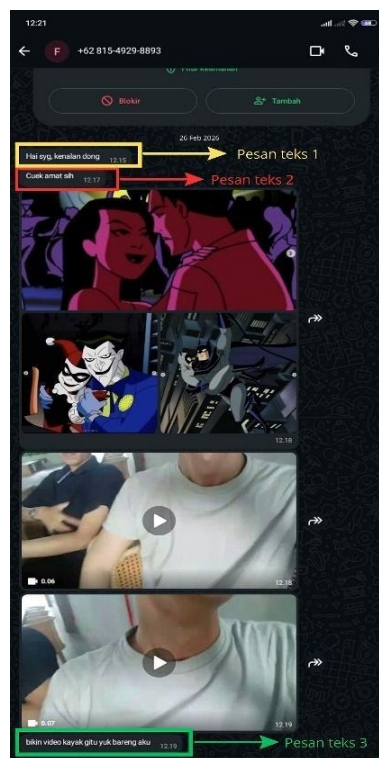


Figure 5. Screenshot of the WhatsApp Conversation on the Victim's Device

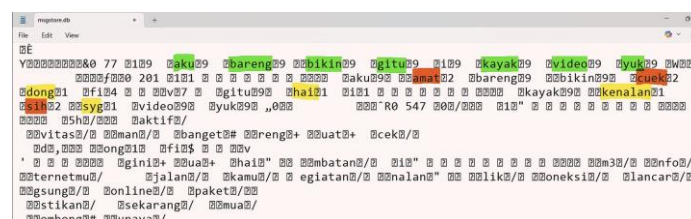


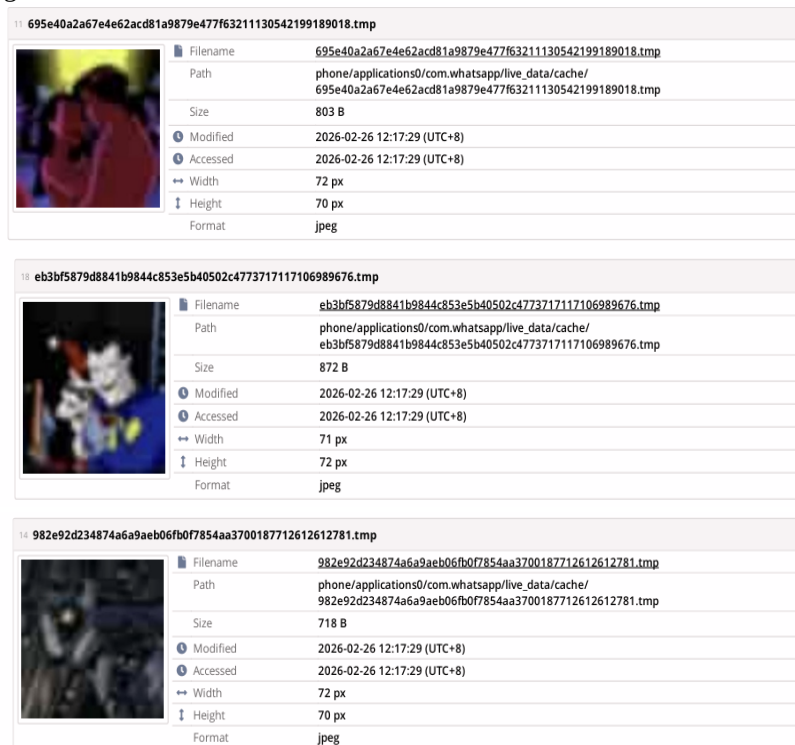
Figure 6. Keyword Fragments in the msgstore.db File

Table 1. Matching the Victim's Evidence with Message Artifacts

No.	Message content	Time (victim)	Fragments (msgstore.db)	Time (Belkasoft, local)	Match
1.	"Hai syg, kenalan dong" <i>English: Hi, sweetheart, let's get to know each other.</i>	26/02/2026 12:15	"hai", "syg", "kenalan", "dong"	26/02/2026 12:15:40	Match
2.	"Cuek amat sih" <i>English: Why are you so indifferent?</i>	26/02/2026 12:17	"cuek", "amat", "sih"	26/02/2026 12:17:13	Match
3.	"bikin video kayak gitu yuk bareng aku" <i>English: Let's make a video like that together.</i>	26/02/2026 12:19	"bikin", "video", "kayak", "gitu", "yuk", "bareng", "aku"	26/02/2026 12:19:42	Match

As shown in Table 1, the matching results demonstrate a perfect logical correlation. The keywords found in the perpetrator's database literally reflect the sentences received by the victim, and the sending timestamps coincide exactly to the same minute and second. This cross-validation approach provides logical and absolute certainty that the communication containing the harassing statements actually occurred, thereby eliminating any opportunity for the perpetrator to deny the events or present an alibi in court.

The next artifacts analyzed were WhatsApp multimedia messages, comprising images and videos identified in the acquisition results. The perpetrator was unaware that the WhatsApp message deletion feature does not immediately eliminate the physical multimedia files previously rendered by the device's system. Using MOBILedit, investigators examined hidden system directories. At the storage path `phone/applications0/com.whatsapp/live_data/cache/`, they successfully located 3 image file artifacts with the `.tmp` extension. Despite their temporary file extension, these files contained complete hexadecimal JPEG image data with pornographic content, together with modification timestamp metadata identical to the sending times of the text messages.

**Figure 7.** WhatsApp Image Artifacts Extracted Using MOBILedit

Subsequently, an in-depth search of the Media/WhatsApp Video/ directory successfully extracted 2 obscene video file artifacts with the `.mp4` extension. Both were recovered in full, together with resolution metadata

(1080x1920 px) and frame rate metadata (25 fps), forensically demonstrating that the files originated from WhatsApp application activity on the perpetrator's device.

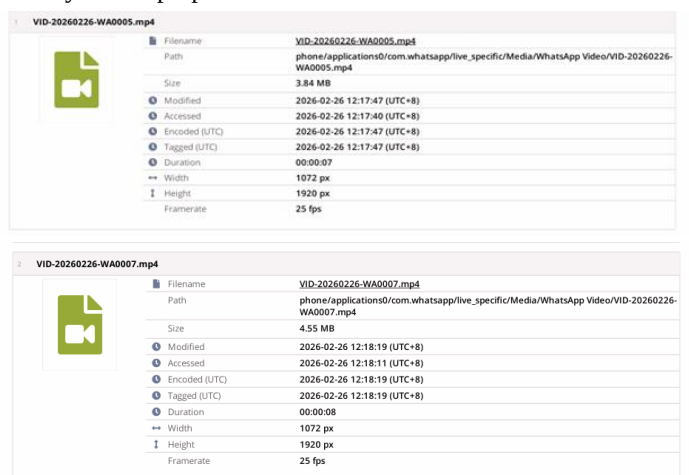


Figure 8. WhatsApp Video Artifacts Extracted Using MOBILedit

D. Reporting

The final stage of the NIST methodology is reporting. All artifacts were objectively summarized for attachment to the official examination report (Berita Acara Pemeriksaan, BAP). The digital evidence successfully collected and verified from the perpetrator's device (Xiaomi Redmi S2) is summarized in Table 2.

Table 2. Summary of Digital Artifact Findings

No.	Application (Object)	Artifact	Number Recovered
		Text Messages	3
		Images	3
		Videos	2

As shown in the summary table, all relevant artifacts were successfully identified, including 3 text message entries marked as deleted but retaining their metadata, along with 3 image artifacts and 2 video artifacts extracted together with their file metadata and associated account identities. Although the text message content could not be displayed because the messages were marked as deleted, the combination of message metadata and multimedia findings can support chronological reconstruction and strengthen the connection between the findings and the case scenario in this study.

The application of the NIST method in this study produced a structured investigative workflow through device isolation using Airplane Mode and controlled acquisition/extraction to maintain digital evidence integrity. These findings are consistent with Kusumadewa et al., who showed that combining NIST with MOBILedit can preserve data authenticity by creating an image file as a preservation measure [16], and with Barkem and Sidabutar, who emphasized the importance of disconnecting the device using Airplane Mode to minimize data changes before acquisition [17].

Attempts to delete messages using Delete for Everyone still left forensic traces, as evidenced by message metadata with an Is Deleted status and the successful extraction of 3 images and 2 videos from application storage. This supports the findings of Karseno and Hendrik that WhatsApp deletion primarily involves system-level marking, while the data may remain on the storage medium [7].

Validation was performed by matching the victim's screenshots, keyword fragments in msgstore.db, and timestamps in Belkasoft metadata. The correlation across sources showed agreement in the keywords and the incident's time frame, strengthening the reliability of the interpretation even though the message content could not be displayed on the sender's device.

The limitations include device conditions that facilitated extraction, namely being powered on and rooted; unstructured msgstore.db fragments without metadata; and the use of the trial version of Belkasoft. Nevertheless, the results remain valuable because they are based on artifacts that can be verified and cross-validated.

IV. Conclusions

This study systematically applied the NIST stages of Collection, Examination, Analysis, and Reporting to acquire and analyze WhatsApp digital evidence. The identified artifacts included deleted text message metadata (Outgoing, Sent, Is Deleted, and timestamps), as well as multimedia artifacts consisting of 3 image files and 2 video files with their file metadata, supporting the reconstruction of media transmission activity in accordance with the case scenario. Future studies are advised to test devices under different conditions, such as non-rooted devices and those with newer security systems; compare other forensic tools or full software versions to strengthen validation; and extend the investigation to instant messaging applications other than WhatsApp to obtain more comprehensive results.

REFERENCES

- [1] I. Zuhriyanto, A. Yudhana, and I. Riadi, "Analisis Perbandingan Tools Forensic pada Aplikasi Twitter Menggunakan Metode Digital Forensics Research Workshop," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 4, no. 5, pp. 829–836, 2020.
- [2] F. Anggraini, Herman, and A. Yudhana, "Analisis Forensik Aplikasi TikTok Pada Smartphone Android Menggunakan Framework Association of Chief Police Officers," *JURIKOM (Jurnal Ris. Komputer)*, vol. 9, no. 4, pp. 1117–1127, 2022, doi: 10.30865/jurikom.v9i4.4738.
- [3] W. A. Social, "Digital 2025 - We Are Social Indonesia," We Are Social. Accessed: Nov. 17, 2025. [Online]. Available: <https://wearesocial.com/id/blog/2025/02/digital-2025/>
- [4] Kementerian Komunikasi dan Informatika RI, "Apresiasi Laporan Masyarakat, Komdigi Tangani Konten Pornografi dan Judi Online," Siaran Pers Kementerian Komunikasi dan Informatika. Accessed: Dec. 05, 2025. [Online]. Available: <https://www.komdigi.go.id/berita/siaran-pers/detail/apresiasi-laporan-masyarakat-komdigi-tangani-13-juta-konten-pornografi-dan-judi-online>
- [5] Pusat Informasi Kriminal Nasional (Pusiknas) Bareskrim Polri, "Waspada! Konten Pornografi Lebih Banyak Disebar di Media Sosial," Pusiknas Polri. Accessed: Dec. 05, 2025. [Online]. Available: https://pusiknas.polri.go.id/detail_artikel/kasus_pat_di_babel:_peringat_tidak_asal_sebarkan_konten_di_media_sosial
- [6] H. Supardin, R. Satra, and M. Arfah, "Analisis Perbandingan Tools Forensik Digital pada Instagram Messenger menggunakan Metode National Institute of Standards and Technology (NIST)," *Bul. Sist. Inf. dan Teknol. Islam*, vol. 3, no. 4, pp. 274–283, 2022.
- [7] D. Karseno and B. Hendrik, "Investigasi dan Analisis Pengembalian Pesan Whatsapp yang Sudah Terhapus Menggunakan Metode National Institute of Justice (NIJ)," *Indones. Res. J. Educ.*, vol. 4, no. 3, pp. 7–12, 2024.
- [8] Rakha Pangestu Raharja, E. I. Alwi, and A. W. M. Gaffara, "Analisis Digital Forensic pada Aplikasi WhatsApp Menggunakan Metode National Institute of Justice (NIJ) pada Smartphone Android," vol. 5, no. 2, pp. 160–168, 2024.
- [9] Nasirudin, Sunardi, and I. Riadi, "Analisis Forensik Smartphone Android Menggunakan Metode NIST dan Tool MOBILedit Forensic Express," *J. Inform. Univ. Pamulang*, vol. 5, no. 1, pp. 89–94, 2020.
- [10] M. Rifqi, S. juli I. Ismail, and M. F. Rizal, "Analisis Forensik Untuk Penanganan Cyber Crime Pada Aplikasi Whatsapp Menggunakan Metode National Institute Of Standard And Technology (Nist Sp 800-86)," *e-Proceeding Appl. Sci.*, vol. 9, no. 6, pp. 3017–3022, 2023.
- [11] A. W. Kusuma, E. I. Alwi, and R. Ramdaniah, "Analisis Bukti Digital Pada Media Penyimpanan Flash Disk Menggunakan Metode National Institute Of Standards And Technology (NIST)," *CyberSecurity dan Forensik Digit.*, vol. 7, no. 1, pp. 18–24, 2024.
- [12] A. Q. I. Hidayat, E. I. Alwi, and A. W. M. Gaffar, "Studi Forensik Digital : Analisis Bukti Video TikTok dengan Metode DFRWS," *J. Minfo Polgan*, vol. 13, no. 1, pp. 1138–1146, 2024.
- [13] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to Integrating Forensic Techniques into Incident Response," Gaithersburg, MD, 2006.
- [14] I. Anshori, N. Sahrun, and Sularno, "Comparative Study of Digital Forensic Techniques : NIJ vs NIST in Digital Data Retrieval," *J. Electr. Eng. Comput. Sci.*, vol. 1, no. 2, pp. 34–40, 2025.
- [15] M. Fitriana, K. AR, and J. M. Marsya, "Penerapan Metode National Institute of Standards and Technology (NIST) Dalam Analisis Forensik Digital Untuk Penanganan Cyber Crime," *Cybersp. J. Pendidik. Teknol. Inf.*, vol. 4, no. 1, pp. 29–39, 2020.
- [16] R. B. Kusumadewa and Z. Sari, "Comparative Analysis of Forensic Digital Evidence on Android Smartphone based Instant Messaging Using NIST Framework," vol. 4, no. 3, pp. 407–422, 2022.
- [17] W. Barkem and J. Sidabutar, "Digital Forensic Analysis of WhatsApp Business Applications on Android Smartphones Using NIST," vol. 22, no. 3, pp. 615–626, 2023, doi: 10.30812/matrik.v22i3.3033.