

Assesing Digital Evidence Availability in Discord Phishing using ISO/IEC 27037 and Anti-Forensics Analysis

Anton Yudhana¹, Zulki Yanto Rivai², Imam Riadi³

¹ Department of Electrical Engineering, Universitas Ahmad Dahlan, Yogyakarta, Indonesia

² Master Program of Informatics, Universitas Ahmad Dahlan, Yogyakarta, Indonesia

³ Department of Information System, Universitas Ahmad Dahlan, Yogyakarta, Indonesia

Article Info

Article history:

Received Jan 19, 2026

Revised Feb 07, 2026

Accepted Feb 24, 2026

Keywords:

Digital Forensics

Phishing Investigation

Discord

ISO/IEC 27037

Digital Evidence Availability

ABSTRACT

Phishing incidents on modern communication platforms pose significant challenges for digital forensics investigations, particularly regarding the availability and preservation of digital evidence. This research aims to evaluate the availability of digital evidence in Discord-based phishing cases by applying the ISO/IEC 27037 framework and interpreting the results from an anti-forensics perspective. This research uses a digital forensics case analysis approach on the victim's mobile device by following the stages of identification, collection, acquisition, and preservation. The results show that of the five types of digital evidence identified, only 40% can be fully preserved, while 20% are partially preserved, and 40% cannot be preserved. The quantitative evaluation produced an average digital evidence availability score of 0.5, indicating that only half of the expected digital evidence could be retained even though the entire forensics procedure had been systematically applied. These findings confirm that the limitations in the availability of digital evidence are influenced not only by the investigation process but also by the technical characteristics of digital artifacts and the system mechanisms inherent to the Discord platform.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Zulki Yanto Rivai,

Master Program of Informatics,

Universitas Ahmad Dahlan,

Jl. Prof. DR. Soepomo Sh, Warungboto, Umbulharjo, Yogyakarta, Indonesia.

Email: 2408048019@webmail.uad.ac.id

1. INTRODUCTION

The rapid adoption of digital communication platforms has transformed social interactions and expanded the scope of cybercrime. Phishing is among the most prevalent threats, exploiting user trust through deceptive messages to steal sensitive information [1], [2], [3], [4], [5], [6]. Recently, platforms like Discord have been misused for phishing due to their real-time communication, cross-platform accessibility, and private messaging [7], [8], [9], [10], [11]. Ars Technica reported that about 70,000 users' government ID were stolen in a large Discord phishing breach, highlighting the real-world consequences of these campaigns [12].

From a digital forensics perspective, phishing incidents on modern communication platforms pose substantial challenges regarding the availability and persistence of digital evidence. Communication artifacts such as chat messages, shared links, and media files are inherently dynamic and may be altered, deleted, or rendered inaccessible by application mechanisms, security policies, or post-incident user activity [13], [14], [15], [16], [17]. As a result, investigators often conduct forensics examinations of devices received after the incident, where portions of potentially relevant evidence may already be partially degraded or entirely unavailable [18], [19], [20], [21].

Previous studies on phishing investigations and instant messaging forensics have primarily focused on artifact extraction techniques, forensics tool capabilities, or attack pattern identification

[22], [23], [24], [25]. While these studies contribute important technical insights, they tend to emphasize the success of evidence acquisition rather than critically examining the conditions under which digital evidence becomes partially available or unavailable, even when forensics procedures are properly applied [26], [27], [28], [29].

To address this research gap, this research proposes an evaluative approach to assessing the availability of digital evidence in Discord phishing investigations by integrating ISO/IEC 27037 with an anti-forensics analytical perspective. In this context, ISO/IEC 27037 is employed to ensure that the stages of identification, collection, acquisition, and preservation are conducted in a forensically sound manner [30], [31], [32], [33], [34]. This standard is particularly relevant for post-incident investigations on instant messaging platforms, where evidence availability is highly dependent on artifact persistence and system behavior at the time of examination [35], [36], [37]. By adopting ISO/IEC 27037, this research ensures that observed evidence limitations can be attributed to inherent technical conditions rather than procedural inconsistencies. Meanwhile, anti-forensics concepts are applied as a post-acquisition interpretative framework to explain evidence limitations, rather than as representations of deliberate actions performed by attackers [38], [39], [40], [41].

The integration of ISO/IEC 27037 with an anti-forensics analytical approach strengthens both the procedural rigor and interpretive depth of digital investigations. This framework enables investigators to assess evidence integrity and persistence across dynamic communication environments such as Discord and Telegram, enhancing post-incident reliability and judicial admissibility. It also supports the development of standardized evaluation criteria for digital evidence quality, promoting cross-jurisdictional cooperation and forensics consistency in cybercrime investigations [42], [43].

The primary contribution and novelty of this research lie in shifting the analytical focus from evidence acquisition success toward understanding the availability and limitations of digital evidence. By classifying forensics artifacts based on concepts such as evidence volatility, persistence selectivity, data persistence, and persistent logical artifacts, this research provides a structured explanation of why certain digital evidence can be preserved while others cannot. Therefore, this research aims to evaluate the availability of digital evidence in Discord phishing investigations through a systematic forensics process, while offering a more realistic interpretation of forensics outcomes on modern communication platforms. The reported availability score and preservation ratios should be interpreted as case-specific indicators rather than generalized benchmarks for Discord phishing investigations.

2. RESEARCH METHOD

This research uses a digital forensics case analysis approach to assess the availability of digital evidence in phishing cases based on the Discord platform. The investigation was conducted after the incident, namely after the victim reported the incident, with a focus on the condition of the digital evidence available when the device was received for examination. The handling of digital evidence is defined by ISO/IEC 27037, which outlines the stages of identification, collection, acquisition, and preservation, as shown in Figure 1. This process is intended to ensure that the investigation process is structured and accountable.



Figure 1. ISO/IEC 27037 Flow

2.1 Research Stage

This research follows the ISO/IEC 27037 framework, which comprises four main stages, as shown in Figure 1, namely identification, collection, acquisition, and preservation. Each stage is carried out sequentially to maintain the integrity and authenticity of digital evidence [44].

1. Identification

The identification stage aims to identify sources of digital evidence related to an event, such as devices, storage media, and associated digital data.

2. Collection

The collection phase is conducted to secure identified digital evidence sources to prevent data alteration or loss prior to the acquisition process.

3. Acquisition

The acquisition stage is the process of copying digital data from evidence sources using appropriate forensics methods. Acquisition is carried out to obtain a representation of the data that can be further analyzed, while maintaining the integrity and authenticity of the original data.

4. Preservation

The preservation stage focuses on maintaining the integrity and validity of the digital evidence obtained. At this stage, evidence is systematically stored and documented, including recording the chain of custody, so that it remains accountable during the analysis and reporting process.

Based on the stages described above, this research applies an ISO/IEC 27037-based digital forensics investigation approach to analyze phishing cases on the Discord platform, focusing on the victim's device. The data obtained through the identification, collection, and acquisition processes is analyzed to evaluate the availability and preservation of digital evidence. All forensics stages and procedures are systematically documented to ensure the validity of the research results and enable replication by subsequent researchers.

2.2 Research Tools and Materials

Several supporting tools are used to support the digital forensics investigation process. The tools and materials used are divided into two categories, namely hardware and software. Table 1 lists the materials and hardware used in this research.

Table 1. Research Tools

No	Device	Operating System	Status	Function
1	Oppo A57	Android 6.0.1	Routed	Research Object
2	Xiomi Redmi 3	Android 7.0.1	Routed	Research Object
3	Laptop Acer	Windows 11 64 bit	RYZEN 3 8.00 GB RAM	Workstation for forensics analysis
4	USB Connector			Connects smartphone to workstation

Next, Table 2 shows the software used as a supporting tool in the forensics investigation process.

Table 2. Supporting Software

No	Device	Version	Function
1	Discord Mobile	279.13	Software test
2	Windows	11	Workstation operating system
3	Oxygen Forensics Detective	17.1.0.131	Forensics & Analysis tool
4	Magnet Axiom	2.4.0.26185	Forensics & Analysis tool
5	Android Debugging Bridge	1.4.3	Connects smartphone to workstation

Table 1 summarizes the hardware components utilized during the forensics examination, including the victim's device and supporting equipment required for data acquisition and preservation. Meanwhile, Table 2 outlines the forensics software tools used for data extraction, analysis, and validation throughout the investigation.

2.3 Research Scenario

This research uses a phishing incident scenario on the Discord platform consisting of seven stages of events leading up to reporting and initial handling by investigators, as illustrated in Figure 2. The scenario begins with message initiation by the perpetrator, followed by receipt of the message by the victim and the victim's interaction with a malicious link. The incident then escalates to loss of account access and subsequent account misuse by unknown parties. Finally, the process continues with incident reporting by the victim and initial handling by investigators.



Figure 2. Research Scenario

Figure 2 shows the research scenario through seven stages that represent the sequence of events in a phishing incident.

1. Message Initiation by Perpetrator

The perpetrator sent Discord messages in a formal, official-sounding style, using language that resembled official communication and including links that claimed to require immediate follow-up.

2. Receipt of Message by Victim

The victim received the message via private message on Discord and initially felt skeptical, but the message's structured, formal tone prompted the victim to pay closer attention.

3. Victim Interaction with the Link

The victim followed the instructions provided by interacting with the included link, as they considered it a normal procedure for Discord account management.

4. Loss of Account Access

After the interaction, the victim was unable to access their Discord account, and attempts to regain access were unsuccessful.

5. Account Misuse by Unknown Parties

The victim's Discord account was then used by other parties to send similar messages to other users, with patterns and language similar to the initial message.

6. Incident Reporting

Victims become aware of account misuse after receiving reports from other users or discovering unknown activity, then report the incident to the authorities.

7. Initial Handling by Investigators

After receiving the report, investigators conduct initial handling by accepting the victim's device as evidence for the forensics investigation, in accordance with applicable procedures.

The research scenario was developed to provide a structured and realistic context for the digital forensics investigation process. The use of this scenario aims to ensure that the research stages, from evidence handling to the analysis of digital evidence availability, can be explained systematically and consistently. In this scenario, the research does not focus on criminal techniques but rather on evaluating the forensics process and the condition of available digital evidence, so that the research results can be understood and replicated in an academic context.

2.4 Research Scope and Limitations

The scope and limitations of this research are summarized to clarify the analysis's focus and ensure consistency with the research objectives. The use of Android 6.0.1 and 7.0.1 reflects a controlled laboratory environment designed to evaluate the availability of digital evidence under defined conditions. Evidence persistence mechanisms may differ significantly in newer Android versions due to changes in sandboxing, encryption, and application data management. Therefore, the findings of this study should be interpreted as a baseline evaluation rather than as a

representation of current Android implementations. A summary of the research scope and limitations is presented in Table 3.

Table 3. Research Scope and Limitations

No	Aspect	Scope and Limitation Description
1	Case Scenario	The research uses a phishing incident scenario on the Discord platform as the context for investigation up to the reporting and initial handling stages, without replicating or analyzing the criminal techniques technically.
2	Device Scope	Forensics analysis is limited to the victim's device as the primary source of evidence; the perpetrator's device is not included in the scope of the investigation.
3	Device Condition	The analyzed devices were rooted to enable advanced forensics access, with the rooting process conducted ethically and in a controlled manner in a research laboratory environment.
4	Platform Scope	Server-side analysis and Discord's internal infrastructure are not included in this research due to limited access.
5	Artifact Scope	The artifacts analyzed are limited to client-side digital evidence, such as application data, media, and metadata available from forensics acquisition.
6	Tool Usage Scope	This research uses more than one forensics tool as an observation instrument to obtain digital evidence, without the intention of comparing the performance or effectiveness between tools.
7	Anti-Forensics Scope	The concept of anti-forensics is not implemented directly, but rather used as an analytical framework to explain the limitations or absence of digital evidence.
8	Analytical Focus	The research focuses on evaluating the availability of digital evidence and its implications for the implementation of ISO/IEC 27037, rather than on identifying the actions or strategies of perpetrators.

Accordingly, the scope and limitations outlined in Table 3 emphasize that the findings should be interpreted within the defined experimental context and are not intended to represent all real-world Discord phishing investigations. As outlined in Table 3, these constraints indicate that this study is designed to examine the investigative process and the condition of digital evidence, employing an anti-forensics perspective solely as an analytical lens to interpret evidence limitations or absence, rather than to replicate offender behavior or to evaluate forensic tool performance. Within this experimental setting, the condition of the examined devices constitutes a key methodological consideration. The devices were configured with root-level access to facilitate deeper forensic examination under controlled laboratory conditions. Such access was adopted as an experimental compromise to maximize artifact retrieval and does not reflect typical real-world seizure scenarios involving non-rooted devices. Accordingly, the findings should be regarded as baseline observations specific to the experimental context, rather than as universally applicable outcomes.

3. RESULTS AND DISCUSSION

The results of the digital forensics investigation are presented in accordance with the ISO/IEC 27037 framework and discussed in the context of the availability of digital evidence, using an anti-forensics perspective as an interpretive framework.

3.1. Identification

At this stage, investigators identify devices and data that may be relevant as digital evidence in the Discord phishing case. The identification process focuses on the victim's devices used to access the Discord application, aiming to determine the types of digital artifacts likely to be directly related to the incident. The artifacts identified include conversation messages, media files such as images, supporting documents such as PDF files, links shared in conversations, and information related to account credentials and account access status.

Identification is based on preliminary information from the victim's report and the established investigation scenario. At this stage, investigators do not yet collect or analyze data; rather, they determine the scope of digital evidence to be handled in the next stage in accordance with the ISO/IEC 27037 framework. This approach aims to ensure that the investigation process focuses on relevant data and avoids unnecessary examination. A summary of potentially relevant digital artifacts identified in the early stages of the investigation is presented in Table 4.

Table 4. Identified Potential Digital Evidence

No	Digital Evidence Type	Description	Expected Quantity
1	Chat Messages	Pesan percakapan terkait insiden	15
2	Image Files	Gambar yang dikirim atau diterima	5
3	Document Files (PDF)	Dokumen yang dibagikan melalui chat	1
4	Shared Links	Tautan yang disertakan dalam pesan	1
5	Account Credentials	Informasi status akses akun	2
Total			24

The quantitative values in Table 4 represent expected artifacts based on scenarios and preliminary information and do not indicate that evidence has been successfully obtained, this will be presented in the acquisition and research results stages.

3.2 Collection

During the collection phase, investigators secure the victim's device as the primary source of digital evidence and prepare it for forensics acquisition. Security measures are taken to maintain the integrity of the evidence by ensuring the device is in a controlled, documented state prior to any further technical interaction. As shown in Figure 3, the victim device used in this research was an OPPO A57. At this stage, the necessary technical preparations were made to support the acquisition process, including isolating the device from the communication network, setting the device's power, and activating the relevant system configurations, including developer options and USB debugging, in accordance with the requirements of the forensics tools used. This collection stage is crucial to ensure that any limitations in digital evidence availability observed in later stages are not caused by improper handling, but rather by inherent technical characteristics of the device and application environment.



Figure 3. Victim device and specification

After technical preparations and device documentation are complete, the device is ready for processing at the acquisition stage. The documentation of device specifications and conditions shown in Figure 3 serves as a reference to ensure the continuity of the investigation process and maintain the integrity of digital evidence in accordance with the ISO/IEC 27037 framework.

3.3 Acquisition

The acquisition stage is carried out to obtain forensic copies of digital data from the victim's device to support the analysis of the availability of digital evidence. The acquisition process is carried out in a forensically sound manner, using multiple forensic tools to ensure the repeatability and consistency of results without modifying the original data. Oxygen Forensics Detective was used to perform logical acquisition focusing on application-level data, including the Discord application sandbox, databases, and associated media files. MAGNET AXIOM was used to extract artifacts at the application and system levels to observe artifact presence and consistency. This research does not aim to compare acquisition depth between tools, but to verify the consistency of evidence availability across different acquisition outputs. Both tools performed logical acquisition without full physical imaging, extraction focused on application sandbox directories, local databases, cache files, and associated metadata. Acquisition using MAGNET

AXIOM in Figure 4. (b) resulted in the extraction of 128,044 digital artifacts on the OPPO CPH1701 device, while acquisition using Oxygen Forensics Detective in Figure 4. (a) resulted in a logical data backup with a total size of 23.9 GB. These results show the scope of data successfully obtained from the victim's device during acquisition, as shown in Figure 4.

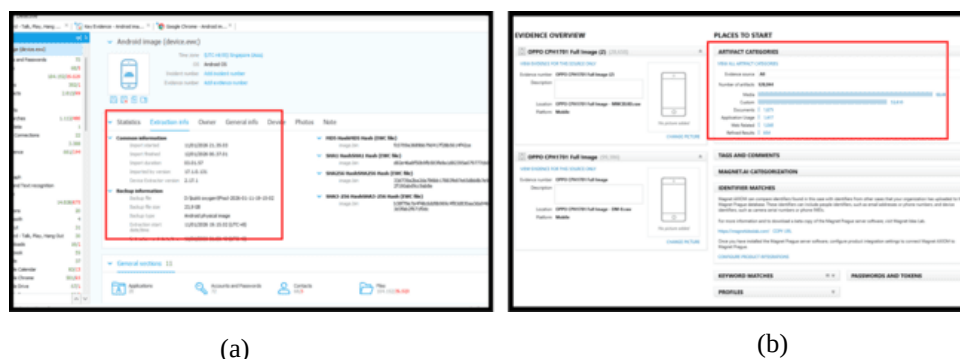


Figure 4. Overview of digital data acquisition results generated by forensics tools.

Acquired artifacts include Discord application data, active communication files, and supporting metadata at the application and system levels. The overview information in Figure 4 is used as a basis for classifying the availability of digital evidence without analyzing the contents of the artifacts. This approach allows the assessment to focus on the presence, consistency, and retrievability of digital evidence rather than its semantic content. As a result, the analysis emphasizes the availability and preservation conditions of evidence, in accordance with the objectives of this research. To present the availability of digital evidence in a concise and structured manner, the acquisition results are summarized in Table 5. Availability status is determined by the consistency of results from each forensics tool used during the acquisition stage. The absence or inconsistency of certain artifacts at this stage indicates that the successful execution of forensic acquisition does not necessarily guarantee the completeness of digital evidence, particularly in cloud-based communication platforms such as Discord.

Table 5. Digital Evidence Availability Summary

No	Evidence Type	Tools A	Tools B	Final Availability
1	Chat Messages	Not Available	Not Available	Not Available
2	Image Files	Available	Not Available	Partially Available
3	Document Files (PDF)	Available	Available	Available
4	Shared Links	Available	Available	Available
5	Account Credentials	Not Available	Not Available	Not Available

As summarized in Table 5, several types of digital evidence differ in availability across forensic tools. This condition is classified as partially available, which indicates inconsistencies in the availability of digital evidence at the acquisition stage. This summary serves as the basis for further discussion of integrity and forensic implications at the preservation stage. These inconsistencies reflect the volatile and selective persistence nature of instant messaging artifacts, where the availability of evidence is influenced by application behavior, synchronization mechanisms, and post-incident system states rather than solely by forensic tool capability.

3.4 Preservation

The preservation stage is the final stage in the ISO/IEC 27037 framework, which aims to maintain the integrity and consistency of digital evidence obtained during the investigation process. In this research, preservation is not only interpreted as a technical safeguarding process, but also as an evaluative stage to assess whether identified digital evidence can realistically be retained throughout the forensic lifecycle. In this research, preservation evaluation was conducted by comparing the digital artifacts identified in the initial stage (Table 4) with the evidence availability

results after the acquisition process (Table 5). This comparison was used not only to determine the final status of digital evidence but also to quantify the levels of availability and preservation. Therefore, the final condition of each type of digital evidence was evaluated using availability scores and preservation ratios as numerical indicators, which were summarized in Table 6.

To enhance methodological clarity and address the derivation of quantitative indicators, this study operationalizes the availability score and preservation ratio as explicit evaluative metrics. These metrics are introduced as an operational definition to formalize commonly reported descriptive evaluations in digital forensic studies, where evidence availability and completeness are typically discussed qualitatively rather than through standardized mathematical formulations [45]. The availability score represents the post-acquisition condition of each identified digital evidence type and is assigned based on its retrievability and consistency across forensic acquisition outputs. A score of 1 indicates full availability, 0.5 indicates partial availability due to incomplete or inconsistent retrieval, and 0 indicates the absence of retrievable evidence. The preservation ratio is derived directly from the availability score to express preservation outcomes in percentage form, enabling clearer interpretation of evidence condition. This condition-based evaluation approach reflects established principles in digital preservation assessment, which emphasize the observable state and integrity of retained digital objects rather than probabilistic assumptions about evidence existence [46]. The preservation ratio for each evidence type is calculated using Equation (1).

$$\text{Preservation Ratio (\%)} = \text{Availability Score} \times 100 \quad (1)$$

To summarize the overall availability condition of digital evidence in the examined case, the arithmetic mean of availability scores across all identified evidence types is calculated, as shown in Equation (2). Each evidence type is treated equally at the category level to represent forensic relevance rather than individual artifact quantity.

$$\text{Average Availability Score} = \frac{\sum_{i=1}^n \text{Availability Score}_i}{n} \quad (2)$$

where *Availability Score* denotes the score assigned to each evidence type and *n* represents the total number of identified evidence types. This operationalization ensures transparency and reproducibility in evaluating digital evidence availability within the ISO/IEC 27037–based forensic investigation framework [47].

To clarify the evaluation process, this study applies a scoring system to represent the post-acquisition condition of digital evidence. The availability score indicates whether each identified evidence type is fully available (score = 1), partially available due to incomplete or inconsistent retrieval (score = 0.5), or unavailable (score = 0). The preservation ratio is derived directly from the availability score and expressed as a percentage to facilitate interpretation of preservation outcomes. This condition-based evaluation reflects the principle that digital evidence preservation is assessed based on the observable state of retained artifacts rather than probabilistic assumptions [46].

Table 6. Digital Evidence Availability and Preservation Assessment.

No	Evidence Type	Expected (Identification)	Acquisition Result	Preservation Status	Availability Score	Preservation Ratio (%)	Anti-Forensics Implication
1	Chat Messages	Yes	Not Available	Not Preserved	0	0%	Evidence volatility
2	Image Files	Yes	Partially Available	Partially Preserved	0.5	50%	Persistence selectivity
3	Document Files (PDF)	Yes	Available	Preserved	1	100%	Data persistence
4	Shared Links	Yes	Available	Preserved	1	100%	Persistent logical artifacts
5	Account Credentials	Yes	Not Available	Not Preserved	0	0%	Credential volatility

Based on the evaluation presented in Table 6, 2 of the 5 identified digital evidence types achieved full preservation, representing 40% of the total evidence types. One evidence type (20%) was partially preserved with an availability score of 0.5, while the remaining two evidence types (40%) were not preserved. The average digital evidence availability score is the arithmetic mean of

the individual availability scores, yielding a value of 0.5. This indicates that, under the examined post-incident conditions, only half of the expected digital evidence could be retained, even though all stages of ISO/IEC 27037 were systematically applied.

In the context of this research, the term anti-forensics is used as a post-acquisition analytical framework to explain the gap between expected digital artifacts and the actual condition of available digital evidence. This approach is not intended to simulate or identify specific actions taken by perpetrators, but rather to analyze the technical characteristics of digital artifacts and system mechanisms that affect the availability and preservation of digital evidence. To summarize the relationship between the stages of ISO/IEC 27037 and the final condition of digital evidence, as summarized in Table 6, a conceptual visualization of the investigation flow and preservation status is presented in Figure 5.



Figure 5. Conceptual overview of investigation stages and digital evidence availability.

The visualization in Figure 5 confirms that the availability status of digital evidence is determined after all stages of ISO/IEC 27037 have been systematically implemented. In the framework of anti-forensic analysis, evidence volatility describes communication artifacts that are temporary and easily lost, while persistence selectivity describes differences in sustainability levels across types of digital artifacts, making some evidence only partially available. Conversely, data persistence describes stable digital artifacts that can be preserved in their entirety, while persistent logical artifacts refer to logical artifacts, such as links or metadata, that tend to remain available during the forensic process. Additionally, credential volatility is used to explain the unavailability of authentication artifacts affected by system security mechanisms, such as session invalidation or credential changes. Thus, the preservation stage not only serves as a process for safeguarding digital evidence but also provides an analytical basis for understanding the variations and limitations in the availability of digital evidence in Discord platform-based phishing case investigations. Thus, the concept of anti-forensics in this research serves as an analytical lens to explain evidence unavailability caused by system-level mechanisms, rather than indicating deliberate evidence manipulation by perpetrators.

4. CONCLUSION

This research shows that applying the ISO/IEC 27037 stages to Discord-based phishing case investigations yields limited digital evidence. Based on quantitative evaluation, only 40% of digital evidence types can be preserved in their entirety, while the rest are partially preserved or unavailable, with an average availability score of 0.5. These findings indicate that the limitations of digital evidence are not solely due to investigative procedures, but also to the technical characteristics of digital artifacts and the system mechanisms inherent to modern communication platforms. Using an anti-forensics perspective as a post-acquisition analysis framework, this research provides a more realistic understanding of the dynamics and limitations of digital evidence availability in forensics investigations on instant messaging platforms.

REFERENCES

- [1] S. L. Sanna, L. Regano, D. Maiorca, and G. Giacinto, "Improving Cybercrime Detection and Digital Forensics Investigations with Artificial Intelligence," 2024, doi: <https://doi.org/10.48550/arXiv.2510.14638>.
- [2] S. Tandel, J. Chordiya, and P. S. H. Patil, "Tricked by the Square : Investigating the Rise and Reach of Quishing Attacks," no. April, 2025, doi: <https://doi.org/10.22214/ijraset.2025.68660>.
- [3] J. B. Vala and V. M. Vekariya, "The Role and Importance of Digital Forensics and Digital Evidence in Cyber Crime Detection," vol. 13, no. 6, pp. 413–420, 2024, doi: https://doi.org/10.69605/ijlbpr_13.6.2024.80.
- [4] S. Ali and M. Yahya, "Social Engineering as an Intermediate Variable between Methods of Persuasion and Electronic Deception from the Point of View of Victims of Cybercrime," vol. 3576, pp. 1013–1026, 2025, doi: <https://doi.org/10.63332/joph.v5i6.2175>.
- [5] P. C. Dave, "Manipulative Communication in Cybercrime : Unraveling the Linguistic," no. 2394, pp. 175–182, 2022, doi: <https://doi.org/10.69758/gimrj/2503i3iivxiiip0031>.
- [6] A. Yudhana, I. Riadi, and S. Suharti, "Network Forensics Against Volumetric-Based Distributed Denial of Service Attacks on Cloud and the Edge Computing," vol. 12, no. 5, pp. 577–588, 2022, doi: <https://doi.org/10.18280/ijssse.120505>.
- [7] K. A. Arifin, "Forensic Analysis of Online Fraud on Telegram Web using Digital Forensics Workshop Method," vol. 187, no. 30, pp. 4–11, 2025, doi: <https://doi.org/10.5120/ijca2025925515>.
- [8] Purwadi, M. Makhfud, and A. Jamaludin, "Research Horizon," vol. 0696, 2025, doi: <https://doi.org/10.54518/rh.5.3.2025.580>.
- [9] A. Mathew and R. Federico, "International Journal of Innovative Research in Science Engineering and Technology (IJIRSET) Phishing 2 . 0 : Leveraging Cyber Threat Intelligence to Combat Deepfake - Enhanced Social Engineering," vol. 14, no. 2, 2025, doi: [10.15680/IJIRSET.2025.1402003](https://doi.org/10.15680/IJIRSET.2025.1402003).
- [10] S. G. A. Rohini, B. Rajashree, and S. S. Sree, "Social Engineering Attacks in Cybersecurity," no. May, 2025, doi: <https://doi.org/10.22214/ijraset.2025.72253>.
- [11] R. Kolandaisamy and H. Rajagopal, "Emergence of Cybercrimes in Online Social Networks," pp. 556–564, 2024, doi: <https://doi.org/10.5954/icarob.2024.os18-11>.
- [12] VELSICURO, "Data 70.000 Pengguna Bocor Akibat Peretasan Server Discord," cyberranges.velsicuro.com. [Online]. Available: <https://cyberranges.velsicuro.com/artikel/data-70000-pengguna-bocor-akibat-peretasan-server-discord>
- [13] V. Kozii and H. Vlasova, "Peculiarities of recording electronic evidence in criminal proceedings regarding crimes committed in Ukraine using cryptocurrencies," vol. 42, no. 42, 2025, doi: <https://doi.org/10.7238/idp.v0i42.429924>.
- [14] M. C. E. Lim *et al.*, "Analysis of Forensic Disk Imaging Tools for Data Acquisition and Preservation," *Journal of Informatics and Web Engineering*, vol. 4, no. 2, 2025, doi: <https://doi.org/10.33093/jiwe.2025.4.2.11>.
- [15] I. Hamid and M. M. H. Rahman, "A Comprehensive Literature Review on Volatile Memory Forensics," 2024, doi: <https://doi.org/10.3390/electronics13153026>.
- [16] I. Riadi, A. Yudhana, and G. P. Inngam Fanani, "Mobile Forensic Tools for Digital Crime Investigation: Comparison and Evaluation," *International Journal of Safety and Security Engineering*, vol. 13, no. 1, pp. 11–19, 2023, doi: [10.18280/ijssse.130102](https://doi.org/10.18280/ijssse.130102).
- [17] M. N. Faiz, "Comparative Analysis of Cloning-Hashing Applications for Securing Digital Evidence," vol. 14, no. 02, pp. 214–220, 2023, doi: [10.35970/infotekmesin.v14i2.1844](https://doi.org/10.35970/infotekmesin.v14i2.1844).
- [18] N. A. Rakha, *Cybercrime and the Law : Addressing the Challenges of Digital Forensics in Criminal Investigations*, vol. XVI, no. June, 2024, doi: <https://doi.org/10.22201/ijj.24485306e.2024.2.18892>.
- [19] M. Raciti, D. Van Landuyt, and G. Bella, "To See or Not to See : A Privacy Threat Model for Digital Forensics in Crime Investigation," 2025 *13th International Symposium on*

- Digital Forensics and Security (ISDFS)*, pp. 1–6, 2025, doi: 10.1109/ISDFS65363.2025.11011965.
- [20] M. Raciti and G. Bella, “Behind the (Digital Crime) Scenes : An MSC Model,” *2024 12th International Symposium on Digital Forensics and Security (ISDFS)*, pp. 1–6, doi: 10.1109/ISDFS60797.2024.10527316.
- [21] R. N. Bintang, R. Umar, and A. Yudhana, “Assess of Forensic Tools on Android Based Facebook Lite with the NIST Method,” *Sci. J. Informatics*, vol. 8, no. 1, pp. 1–9, 2021.
- [22] R. S. Santos, “Advanced Research on Information Systems Security Digital Forensics on Trending Technologies : A systematic Literature Review,” vol. 4, no. 2, pp. 4–15, doi: <https://doi.org/10.56394/aris2.v4i2.40>.
- [23] N. Yalçın and T. Yıldırım, “Logical Image Acquisition and Analysis of Android Smartphones,” pp. 139–152, 2024, doi: 10.4236/jcc.2024.124011.
- [24] N. Anwar, “Comparative Analysis of NIJ and NIST Methods for MicroSD Investigations : A Technopreneur Approach,” vol. 6, no. 2, pp. 169–181, 2024, doi: <https://doi.org/10.34306/att.v6i2.407>.
- [25] W. A. Baroto, “Asia Pacific Fraud Journal,” vol. 9, no. 1, pp. 1–16, 2024, doi: 10.21532/apfjournal.v9i1.346.
- [26] O. S. Igonor and M. B. Amin, “The Application of Blockchain Technology in the Field of Digital Forensics : A Literature Review,” 2025, doi: <https://doi.org/10.3390/blockchains3010005>.
- [27] N. ali Suleiman, “Deepfake-as-a-Service : The Next Challenge for Enterprise Cybersecurity Deepfake-as-a-Service : The Next Challenge for Enterprise Cybersecurity,” vol. 7, no. 3, pp. 47–59, 2025, doi: <https://doi.org/10.47941/jts.2752>.
- [28] M. Ashawa, A. Mansour, J. Riley, J. Osamor, and N. P. Owoh, “Digital Forensics Challenges in Cyberspace : Overcoming Legitimacy and Privacy Issues Through Modularisation,” pp. 140–156, 2023, doi: <https://doi.org/10.37256/ccds.5120233845>.
- [29] A. Yudhana, “Live Forensic Environment with Parallel Data Acquisition for Investigating Private Mode Browsing,” vol. 13, no. 3, pp. 577–585, 2023.
- [30] A. Faizal and A. Luthfi, “Comparison Study of NIST SP 800-86 and ISO/IEC 27037 Standards as A Framework for Digital Forensic Evidence Analysis,” *Journal of Information Systems and Informatics*, vol. 6, no. 2, pp. 701–718, 2024, doi: 10.51519/journalisi.v6i2.717.
- [31] A. R. Fakhriansyah and A. Luthfi, “Development of Xiaomi Product Mobile Forensic Acquisition Framework on Second Space Features Based on SNI / ISO,” pp. 255–272, 2024, doi: <https://doi.org/10.20895/infotel.v16i2.1091>.
- [32] E. Hafidy, P. Siber, P. Siber, H. Kabetta, P. Siber, and P. Siber, “Digital Artifact Analysis on Windows Subsystem for Android (WSA) based on ISO / IEC 27037 : 2012 and ISO / IEC 27042 : 2015,” *2024 IEEE 2nd International Conference on Electrical Engineering, Computer and Information Technology (ICEECIT)*, pp. 41–46, 2024, doi: 10.1109/ICEECIT63698.2024.10859797.
- [33] R. A. Ramadhan, P. R. Setiawan, and D. Hariyadi, “Digital Forensic Investigation for Non-Volatile Memory Architecture by Hybrid Evaluation Based on ISO / IEC 27037 : 2012 and NIST SP800-86 Framework,” vol. 6, no. 2, pp. 162–168, 2022, doi: <https://doi.org/10.25299/itjrd.2022.8968>.
- [34] H. Yang, I.-L. Hung, and Y. Chao, “Enhancing Traditional Reactive Digital Forensics to a Proactive Digital Forensics Standard Operating Procedure (P-DEFSOP) : A Case Study of DEFSOP and ISO 27035,” pp. 1–18, 2025, doi: <https://doi.org/10.3390/app15189922>.
- [35] A. O. Felix, “Enhancing Digital Forensics Investigations Using AI Driven Anomaly Detection and Log Correlation : A Mixed Methods Approach Article Info Issue : 04 July – August 2025 Received : 23-05-2025 Accepted : 24-06-2025 Page No : 71-84,” pp. 71–84, 2025, doi: <https://doi.org/10.54660/ijfei.2025.2.4.71-84>.

- [36] S. Rudrakar, P. Rughani, and L. Sadineni, "Digital forensics and incident response management model for IoT based agriculture," no. 2025, pp. 1–23, 2027, doi: <https://doi.org/10.1038/s41598-025-02635-2>.
- [37] M. S. Zareen, B. Aslam, S. Tahir, and I. Rasheed, "Unveiling the Dynamic Landscape of Digital Forensics : The Endless Pursuit," pp. 1–34, 2024, doi: <https://doi.org/10.3390/computers13120333>.
- [38] S. Surakanti, S. Goundar, and J. Dwight, "Countering anti-forensic tactics in cybercrime investigations – a systematic literature review," 2025, doi: <https://doi.org/10.1007/s10207-025-01131-y>.
- [39] P. Narasimhan and N. Kala, "From Evidence to Insight : AI in Digital Forensics," pp. 2198–2203, 2024, doi: <https://doi.org/10.32628/cseit2410612419>.
- [40] I. B. Луцкий, "Problematic Issues of Definition of Digital Forensics," pp. 135–160, 2023, doi: [10.21564/2225-6555.2023.23.281734](https://doi.org/10.21564/2225-6555.2023.23.281734).
- [41] N. A. Almubairik, "Systematic Literature Review on Wearable Digital Forensics : Acquisition Methods , Analysis Techniques , Tools , and Future Directions," *IEEE Internet Things J.*, vol. 12, no. 2, pp. 1320–1342, 2025, doi: [10.1109/JIOT.2024.3485027](https://doi.org/10.1109/JIOT.2024.3485027).
- [42] I. S. Said, G. G. Ocen, M. Ali, and A. A. Egwar, "Digital Evidence Lifecycle Management Framework in Courts of Law (DELM-C) : A Case of Zanzibar High Courts," 2025, doi: [10.32604/jcs.2025.066979](https://doi.org/10.32604/jcs.2025.066979).
- [43] F. Caldeira and T. Cruz, "A Survey on Forensics and Compliance Auditing for Critical Infrastructure Protection," no. November 2023, pp. 2409–2444, 2024, doi: <https://doi.org/10.1109/access.2023.3348552>.
- [44] S. A. Hanna, R. Imam, and Sunardi, "Improving Credibility of Digital Evidence Investigation in E- Commerce Fraud Cases using ISO / IEC 27037," *International Journal of Advances in Data and Information Systems*, vol. 6, no. 2, pp. 479–495, 2025, doi: [10.59395/ijadis.v6i2.1408](https://doi.org/10.59395/ijadis.v6i2.1408).
- [45] A. K. Verma and K. Ramanathan, "Data privacy preservation in digital forensics investigation," in *AIP Conference Proceedings*, 2022, p. 030051. doi: [10.1063/5.0109813](https://doi.org/10.1063/5.0109813).
- [46] S. Abrams, "Tacit attitudinal principles for evaluating digital preservation success," *Archival Science*, vol. 21, no. 3, pp. 295–315, Sep. 2021, doi: [10.1007/s10502-021-09360-5](https://doi.org/10.1007/s10502-021-09360-5).
- [47] R. Stoykova and K. Franke, "Reliability validation enabling framework (RVEF) for digital forensics in criminal investigations," *Forensic Science International: Digital Investigation*, vol. 45, p. 301554, Jun. 2023, doi: [10.1016/j.fsidi.2023.301554](https://doi.org/10.1016/j.fsidi.2023.301554).