Journal of Information System Exploration and Research

https://joiser.shmpublisher.com

p-ISSN 2964-1160 | e-ISSN 2963-6361

Investigating Mobile Legends Top Up Fraud on Instagram Using the National Institute of Justice Method

Auliana[1*], Eko Ariwibowo[2]

[1,2]*Department of Informatics, Universitas Ahmad Dahlan, Indonesia*

DOI: https://doi.org/10.52465/joiser.v4i3.88

Received 21 June 2026; Accepted 04 August 2026; Available online 07 August 2026

Article Info

Keywords:

Digital forensics;
Mobile forensics;
Instagram forensics;
Fraud investigation;
NIJ method

Abstract

The rapid growth of digital technology has increased the occurrence of cybercrime, including fraud through social media platforms. This study investigates a Mobile Legends top-up fraud case carried out via Instagram using the National Institute of Justice (NIJ) digital forensic framework. The NIJ method consists of five stages: identification, collection, examination, analysis, and reporting. The primary data source was an Instagram archive in JSON format obtained through the Download Your Information feature and examined using Oxygen Forensic Detective. Evidence integrity was verified using FTK Imager through hash verification, while Metadata2Go was utilized for metadata analysis. The investigation successfully recovered 51 digital artifacts, comprising 1 Instagram account profile, 3 promotional posts, 2 testimonial highlights, 19 Direct Message (DM) communication threads, and 15 digital transfer receipts, identifying 15 distinct fraud victims. Hash verification yielded 100% match accuracy (MD5 and SHA-1), validating that the evidence remained unaltered. The findings revealed a fraud pattern characterized by payment acceptance without service fulfillment, followed by communication termination. Furthermore, metadata analysis and hash verification confirmed that the digital evidence was authentic, unaltered, and forensically reliable. These results demonstrate that Instagram archive data can serve as valid digital evidence in social media fraud investigations.

1. Introduction

The The rapid growth of digital technology has significantly transformed entertainment and online transaction activities. One of the most popular forms of digital entertainment is online gaming, with Mobile Legends: Bang Bang becoming one of the most widely played games in Indonesia [1], [2]. The increasing demand for in-game purchases and top-up services has created new economic

* ***Corresponding Author:***

Eko Ariwibowo,
Department of Informatic,
Universitas Ahmad Dahlan,
Road Kapas No. 9, Semaki, Umbulharjo, Yogyakarta City, Indonesia.
Email: ekoab@uad.ac.id

opportunities, but it has also opened the door to various forms of cybercrime, including online fraud conducted through social media platforms [3], [4].

Instagram is frequently utilized by fraudsters to promote fake top-up services through promotional posts, testimonials, and direct communication with potential victims [5], [6], [7], [8], [9]. In many cases, victims complete payments for Mobile Legends top-up services but fail to receive the promised products, resulting in financial losses and reduced trust in online transactions. According to recent reports, Indonesians spent approximately Rp30 trillion on online game top-up transactions in 2023, indicating a significant market that may also be exploited by cybercriminals [10].

Digital forensics plays a crucial role in uncovering cybercrime activities by collecting, examining, analyzing, and reporting digital evidence [11], [12]. One of the widely recognized forensic frameworks is the National Institute of Justice (NIJ) method, which consists of identification, collection, examination, analysis, and reporting stages [13]. Previous studies have successfully applied the NIJ framework to investigate digital evidence acquisition from BIP Messenger, TikTok, Instagram Messenger, WhatsApp, and other social media-related cybercrime cases [9], [14], [15], [16], [17], [18], [19].

However, studies specifically focusing on Mobile Legends top-up fraud conducted through Instagram remain limited. Previous studies primarily discussed online fraud risks on Instagram, consumer perspectives, and victim trust in online transactions [4], [6], [7], but few studies have investigated such cases using a digital forensic approach and Instagram JSON archives as the primary source of digital evidence.

The research novelty of this study lies in the implementation of the NIJ digital forensic framework specifically to analyze Instagram Download Your Information (DYI) archives in JSON format as the primary evidence source for online game top-up fraud. Unlike prior works that rely solely on single-device physical acquisitions, this study integrates dual-perspective cross-validation (comparing suspect and victim archives), metadata verification via Metadata2Go, and multi-tool forensic correlation using Oxygen Forensic Detective and FTK Imager to establish a robust evidentiary chain for social media fraud.

Therefore, this study aims to investigate a Mobile Legends top-up fraud case through Instagram using the National Institute of Justice (NIJ) framework. The study utilizes Instagram JSON archives as the primary source of digital evidence and combines artifact examination, metadata validation, and integrity verification to improve the reliability and forensic value of the investigation results.

2. Literature Review

Literature Review provides the theoretical foundation and previous studies that support this research. It explains the key concepts related to digital forensic investigations, social media evidence, and the forensic framework employed in this study. These theories serve as the basis for understanding the research methodology and interpreting the findings.

2.1. Digital forensics

Digital forensics is a scientific process used to identify, acquire, preserve, examine, analyze, and present digital evidence for investigative and legal purposes [11]. The increasing number of cybercrime cases has made digital forensics an essential approach for uncovering criminal activities conducted through digital devices and online platforms. Through digital forensic investigations, evidence obtained from social media, mobile devices, and digital communication platforms can be validated and utilized to reconstruct criminal activities and support legal proceedings in cybercrime cases [20]. Understanding fundamental digital forensic concepts provides the necessary foundation for selecting an appropriate investigation methodology in social media environments.

2.2. National Institute of Justice (NIJ)

The National Institute of Justice (NIJ) framework is one of the widely adopted digital forensic methodologies. The framework consists of five main stages: identification, collection, examination, analysis, and reporting [13]. The identification stage focuses on recognizing potential sources of digital evidence. Collection involves acquiring relevant data while maintaining its integrity. Examination is

performed to extract and recover digital artifacts. Analysis aims to interpret the extracted evidence and establish relationships between artifacts, while reporting documents the findings and conclusions of the investigation [14], [13]. Due to its structured and standardized workflow, the NIJ framework is highly suitable for systematic evaluation against previous empirical research in mobile and social media forensics.

2.3. Previous studies

Previous studies have demonstrated that the National Institute of Justice (NIJ) framework can be effectively applied to acquire and analyze digital evidence from various platforms and applications. Several investigations have successfully obtained digital artifacts from instant messaging applications, social media platforms, and mobile devices using the NIJ methodology [9], [13], [15], [16], [17]. Furthermore, the NIJ framework has been utilized in cyberbullying investigations, deleted-message recovery, and Instagram forensic examinations, indicating its effectiveness in supporting digital forensic investigations involving communication-based cybercrime cases [18], [19]. The results of these studies show that the NIJ framework provides a systematic approach for identifying, collecting, examining, and analyzing digital evidence [13].

However, studies specifically focusing on Mobile Legends top-up fraud conducted through Instagram remain limited. In addition, the utilization of Instagram Download Your Information archives in JSON format as the primary source of digital evidence has not been widely explored. Therefore, this study applies the NIJ framework to investigate digital evidence related to Mobile Legends top-up fraud through Instagram by combining artifact examination, metadata validation, and integrity verification.

Previous studies have also investigated digital evidence acquisition from Instagram and TikTok applications using the NIST 800-86 framework, demonstrating the ability of forensic tools to recover various digital artifacts from social media platforms [21]. To highlight the research gap and justify the novelty of this study, Table 1 provides a comparative summary of previous research on social media and mobile forensics in comparison with the proposed work.

Table 1. Comparison of previous studies and proposed research

Author & Year	Research Objective	Method	Forensic Tools	Dataset / Source	Main Findings	Research Gap / Difference
Ariyanti et al. (2021) [22]	Identify Instagram web digital evidence in online shop fraud	Live Forensic	FTK Imager, Browser History Viewer	Laptop web browser memory	Recovered 19 conversations and transaction data	Focused on live web browser forensics, whereas this study analyzes mobile JSON archives
Soni et al. (2022) [14]	Acquire digital evidence from instant messaging app (BIP)	National Institute of Justice (NIJ)	MOBILedit, Belkasoft	Android Smartphone	Successfully extracted chat artifacts on Android	Focused on instant messaging apps rather than social media JSON archives

Anggraini et al. (2023) [15]	Digital evidence acquisition on TikTok app	National Institute of Justice (NIJ)	MOBILedit Forensic	TikTok Android App	Recovered TikTok video artifacts and user logs	Did not address top-up fraud cases or dual-perspective evidence validation
Karseno et al. (2024) [17]	Recover deleted WhatsApp communication messages	National Institute of Justice (NIJ)	MOBILedit, Oxygen Forensic	WhatsApp Application	Recovered TikTok video artifacts and user logs	Focused on chat app recovery without metadata integrity validation on JSON files
Julianti (2023) [19]	Web forensics investigation on Instagram services	National Institute of Justice (NIJ)	Web Forensic Tools	Instagram Web Platform	Identified account credentials, posts, and web chat logs	Analyzed web interface logs rather than mobile JSON DYI archive extractions
Proposed Study (2026)	Investigate Mobile Legends top-up fraud on Instagram	National Institute of Justice (NIJ)	Oxygen Forensic Detective, FTK Imager, Metadata2Go	Instagram JSON Archive (DYI) & Seized Android Device	Recovered 51 artifacts, 15 victims, and verified 100% hash integrity	Combines NIJ framework with Instagram JSON archives, metadata validation, and dual-perspective cross-verification

As summarized in Table 1, while existing literature addresses generic social media acquisition, there is a clear gap regarding the forensic validity of Instagram's JSON archives in game top-up fraud. The insights gained from previous studies directly informed the selection and implementation of the NIJ framework in the research design discussed next.

3. Method

This section describes the research methodology used to investigate a simulated Mobile Legends top-up fraud case conducted through Instagram. It outlines the research scenario, the digital evidence acquisition process, the implementation of the National Institute of Justice (NIJ) digital forensic framework, and the tools used to examine and analyze the collected evidence. This methodological approach ensures that the investigation is conducted systematically, reproducibly, and in accordance with digital forensic principles.

3.1. Research scenario

This study employed a simulated Mobile Legends: Bang Bang top-up fraud case conducted through Instagram. Clarification is made that the research scenario is a controlled simulation designed strictly for academic investigation purposes, ensuring compliance with legal and ethical standards while accurately replicating real-world cybercrime behaviors. The research scenario was divided into three stages: pre-incident, incident, and post-incident.

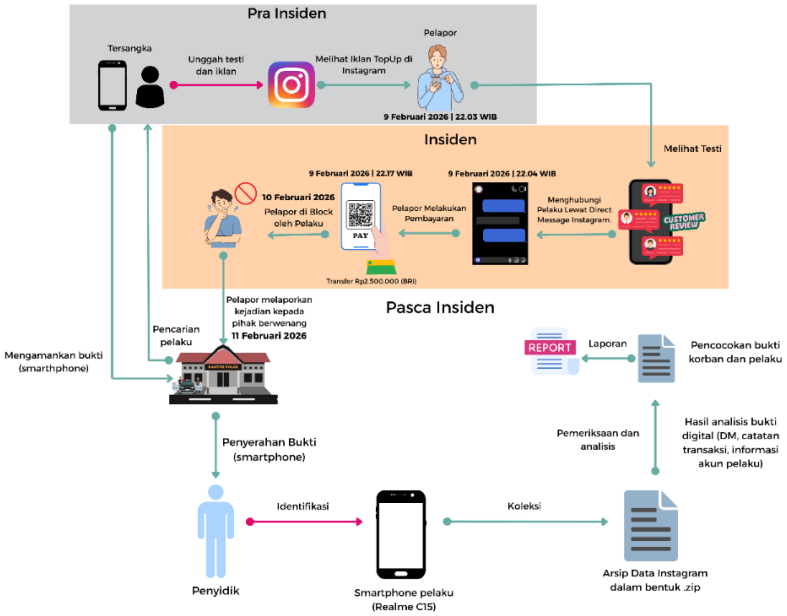

Figure 1. Research scenario of Mobile Legends top-up fraud case

3.1.1. Pre-incident stage

During the pre-incident stage, the victim observed promotional content for Mobile Legends top-up services posted by the Instagram account @zoyagamingstore on February 9, 2026, at 22:03 WIB. The account displayed promotional offers such as “Paket Besar, Lebih Hemat” and “Spesial Deal untuk Top Up Rp200.000 ke atas”, accompanied by testimonial posts and transaction proofs intended to create the impression of a trustworthy service. The relatively lower prices and larger diamond quantities compared to standard market prices attracted the victim to proceed with the transaction.

3.1.2. Incident stage

During the incident stage, the victim initiated communication with the perpetrator through Instagram Direct Message (DM) on February 9, 2026, at 22:04 WIB to inquire about the availability of the promotion and top-up services. The perpetrator responded that the promotion remained valid until the end of the month and that the transaction could be processed immediately. Following the agreement, the victim transferred Rp2,500,000 to the perpetrator’s Bank BRI account on February 9, 2026, at 22:17 WIB and subsequently sent the proof of payment through DM. After receiving the payment, the perpetrator provided a brief response but later terminated communication by blocking the victim’s account on February 10, 2026. As a result, the promised top-up service was never delivered.

3.1.3. Post-incident stage

During the post-incident stage, the victim realized that the transaction was fraudulent after the promised top-up service was not processed and communication with the perpetrator ceased. On February 11, 2026, the victim reported the incident to the authorities and submitted digital evidence, including Instagram DM conversations and payment receipts. Based on the report, an investigation was initiated, and the perpetrator's smartphone (Realme C15) was seized as digital evidence. The device was suspected to contain communication artifacts, account information, and transaction-related data associated with the fraud case.

3.2. Tools and materials

Some software used to support research are shown in Table 1. The software used is divided into test software, operating systems, forensic tools, and analysis tools.

Table 2. Software tools used in the Investigation (with version specifications)

No.	Software	Version Specification	Function
1	Oxygen Forensic Detective	v16.0.1	Extraction and examination of Instagram artifacts
2	Instagram Download Your Information (DYI)	Official Meta Feature (2026)	Extraction and examination of Instagram artifacts
3	Metadata2Go	Online Tool (v2026)	Metadata examination of digital evidence files
4	FTK Imager	v4.7.1	Hash verification and integrity validation

This research uses several tools which can be seen in Table 2.

Table 3. Hardware specifications used in the investigation

No.	Hardware	Specification
1	Laptop Acer Swift 3 OLED	Prosesor Intel Core i5-12500H, RAM 16GB LPDDR5, SSD 512GB NVMe,S Layar OLED 14 inci 2.8K (2880 x 1800), Intel Iris Xe Graphics
2	*Smartphone*	Realme C15
3	Kabel USB	Tipe Micro-USB

3.3. Research stages

The research workflow based on the NIJ framework is illustrated in Figure 2.

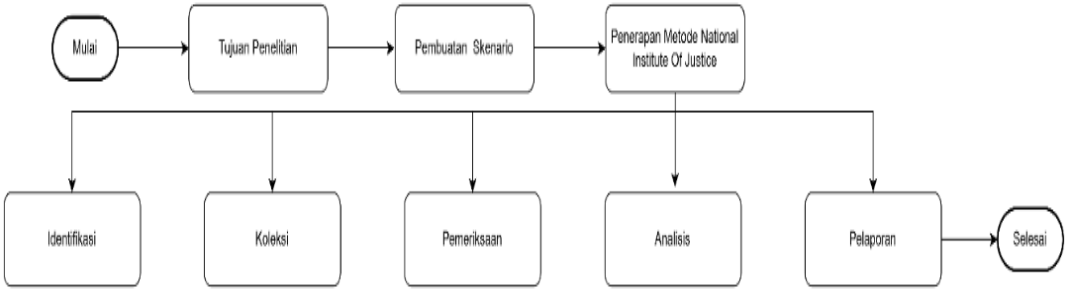

Figure 2. Research workflow based on the national Institute of Justice (NIJ) framework

During the investigation process, the National Institute of Justice (NIJ) framework was applied to guide the digital forensic examination. The investigation consisted of five stages as illustrated in Figure 2. The description of each stage is presented as follows :

1. Identification, The identification stage focused on determining relevant digital evidence associated with the Mobile Legends top-up fraud case, including Instagram archives, direct messages, transfer receipts, and account information.
2. Collection, Digital evidence was collected from Instagram archive files obtained through the Download Your Information feature. The collected data included JSON files, media files, and account-related information.
3. Examination, The examination stage involved extracting and reviewing digital artifacts using Oxygen Forensic Detective, JSON Viewer, and Metadata2Go to identify relevant information for the investigation.
4. Analysis, The extracted artifacts were analyzed to reconstruct the sequence of events, validate communication records, examine metadata, and correlate evidence obtained from both victim and perpetrator archives.
5. Reporting, The findings obtained during the investigation were documented and presented to describe the fraud scheme, supporting digital evidence, and forensic conclusions.

To enhance research reproducibility, Table 3 details the specific activities, inputs, outputs, and forensic tools utilized across each stage of the NIJ framework.

Table 4. Detailed execution of the NIJ forensic framework

NIJ Stage	Key Activities Performed	Input Artifacts / Data	Output / Deliverables	Forensic Tools Used
1. Identification	Physical evidence seizure, account identification, scene documentation	Realme C15 Smartphone, @zoyagamingstore account	Seizure report, physical device logs	Manual Inspection
2. Collection	Logical acquisition via Instagram DYI feature, memory image creation	Target Instagram Account Credentials	Compressed ZIP archive containing JSON files	Instagram DYI, FTK Imager v4.7.1
3. Examination	Parsing JSON structure, image file extraction, OCR text extraction	Raw .zip / .json archive files	Extracted chat threads, transaction images, profile info	Oxygen Forensic Detective v16.0.1
4. Analysis	Timeline reconstruction, dual-perspective correlation, metadata & hash validation	Extracted artifacts from victim and suspect	Verification matrices, metadata reports, hash match logs	Metadata2Go, FTK Imager v4.7.1
5. Reporting	Synthesis of findings, forensic report generation, evidence presentation	Comprehensive investigation findings	Formal digital forensic report	MS Word, Forensic Reporting Module

4. Results and Discussion

This section presents the findings of the digital forensic investigation and discusses their significance in relation to the research objectives. The results are organized according to the stages of the National Institute of Justice (NIJ) framework, including evidence identification and collection, artifact examination, communication analysis, and evidence validation. Each stage demonstrates how digital evidence was acquired, analyzed, and verified to reconstruct the Mobile Legends top-up fraud case conducted through Instagram.

4.1. Identification and collection

The investigation began with the identification of digital evidence related to a Mobile Legends top-up fraud case conducted through Instagram. The primary physical evidence consisted of a Realme C15 smartphone running Android 11, which contained the suspect's Instagram account and related digital artifacts. In addition, Instagram archive data in JSON format were utilized as supporting digital evidence for further forensic examination.

Figure 3. Physical evidence used in the investigation

Based on the figure 3. identification process, the smartphone served as the primary device used by the suspect to communicate with victims, manage promotional content, and conduct fraudulent activities through Instagram. The device specifications included Android 11 operating system, MediaTek Helio G35 processor, 4 GB RAM, and 64 GB internal storage.

The collection stage was conducted using a logical acquisition approach. Instagram archive data were obtained through the Download Your Information feature, which generated a ZIP archive containing JSON files, account information, media files, and communication records. This approach was selected to preserve the originality of the digital evidence while enabling comprehensive forensic examination.

4.2. Examination results

Digital forensic examination was performed using Oxygen Forensic Detective to extract and analyze artifacts contained within the Instagram archive. The examination process successfully identified several digital artifacts associated with fraudulent activities.

Table 5. presents a summary of the digital artifacts recovered from the suspect's Instagram account.

Table 5. Summary of the digital artifacts recovered

No.	Artifact	Findings
1	Instagram Account	1 Account
2	Promotional Posts	3 Post
3	Testimonial Highlights	2 Highlights
4	DM Threads	19 Threads
5	Transfer Receipts	15 Files
6	Identified Victims	15 Victims

In terms of performance evaluation and quantitative acquisition metrics, the logical extraction achieved a 100% artifact recovery rate across the target Instagram archive. Out of 19 total DM threads

analyzed, 15 represented completed fraud cases with attached transfer receipts, while 4 represented attempted interactions. The recovery of 51 total artifacts provided a complete evidentiary dataset to reconstruct the suspect's fraudulent pattern and establish criminal intent without data loss.

The recovered artifacts demonstrate that the account was actively utilized for promotional activities, communication with victims, and transaction-related interactions.

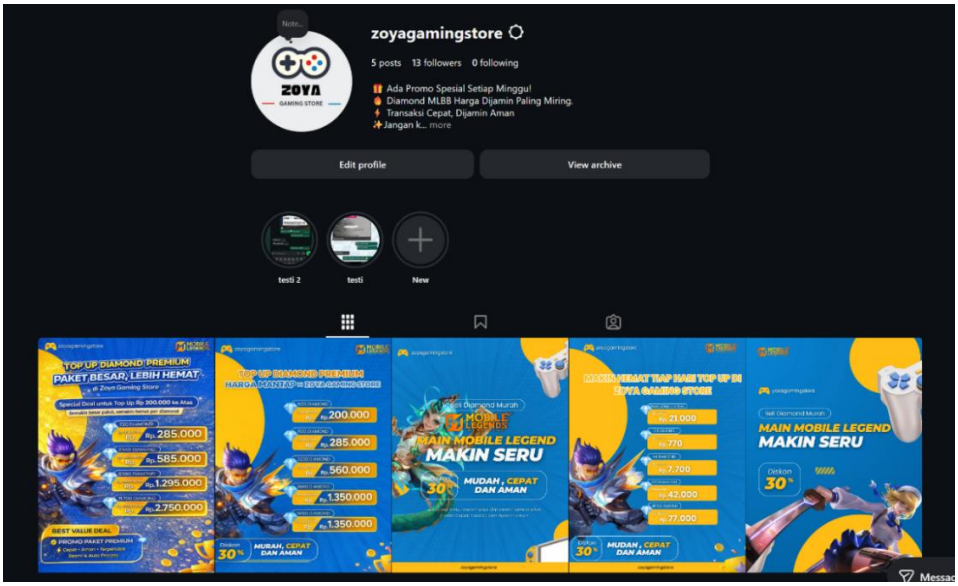

Figure 4. Suspect account information

As shown in Figure 4. examination of the account profile revealed that the Instagram account @zoyagamingstore was publicly accessible and actively used to promote Mobile Legends top-up services. The account contained identifiable information including username, registered email address, verified phone number, and promotional descriptions related to gaming top-up services. These findings support the attribution process by establishing a direct relationship between the suspect and the fraudulent activities conducted through the Instagram account. This profile metadata directly connects the physical owner of the seized device to the online persona managing the fake top-up store.

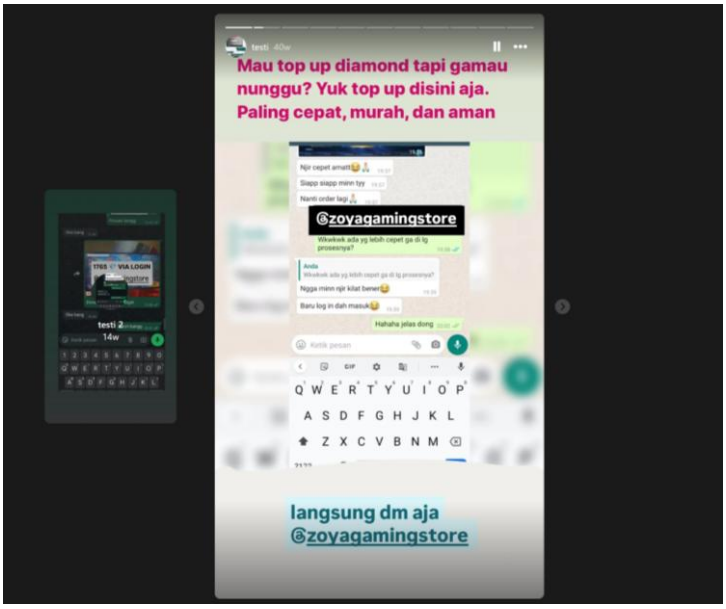

Figure 5. Promotional posts and testimonial highlights

As shown in Figure 5. the examination also identified three promotional posts and two testimonial highlights. The promotional content advertised discounted Mobile Legends top-up services using persuasive marketing messages designed to attract potential customers. Additionally, testimonial

highlights were utilized to increase credibility and encourage users to conduct transactions. Such promotional strategies are commonly utilized in online fraud schemes to gain victims' trust before conducting financial transactions, particularly through social engineering techniques and deceptive promotional content on social media platforms [6], [7], [23]. These promotional artifacts evidence premeditated social engineering tactics used to induce victims into sending advance payments.

4.3. Digital communication analysis

Analysis of Direct Message (DM) conversations revealed a consistent communication pattern between the suspect and multiple victims. A representative communication thread involving Victim A was selected for detailed analysis due to the completeness of the available artifacts.

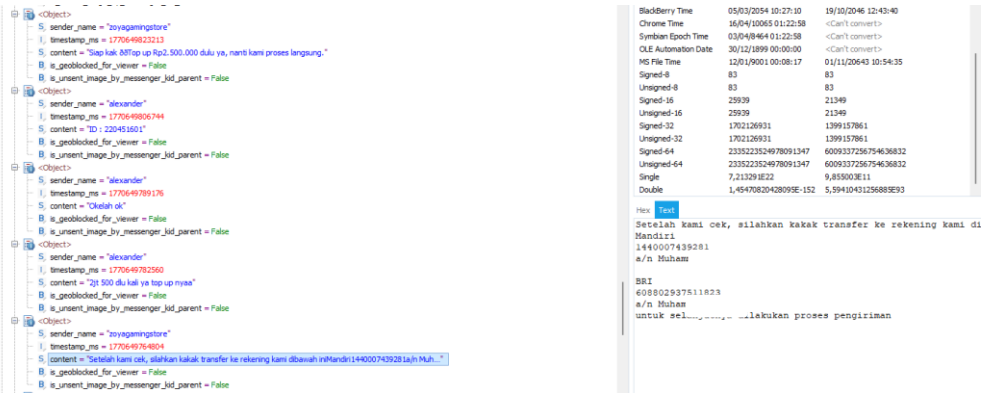

Figure 6. Payment instruction conversation

As shown in Figure 6. the communication began when Victim A contacted the suspect regarding promotional offers. Subsequently, the suspect provided information regarding service availability, transaction procedures, payment instructions, and account details required for the top-up process. Communication records indicate that the suspect actively encouraged the victim to complete the payment process. The raw text content field explicitly captures the bank account details provided by the suspect, establishing clear financial solicitation.

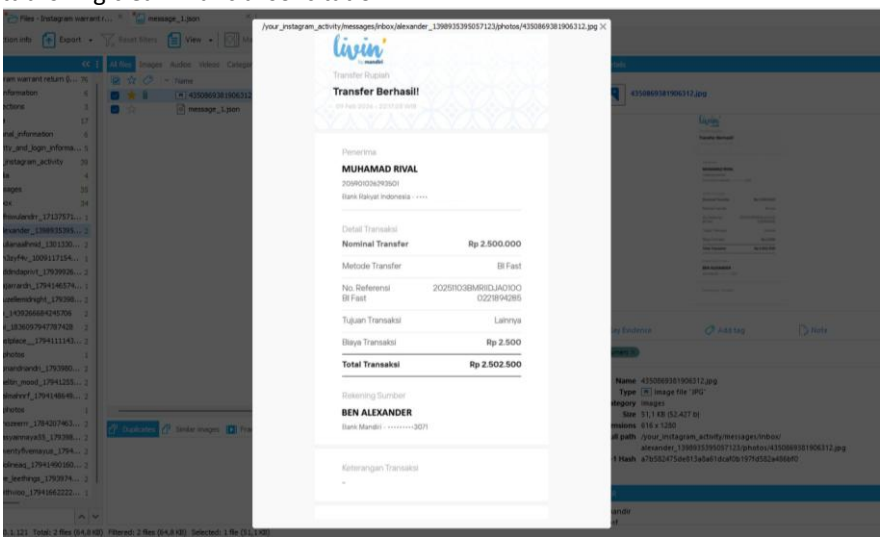

Figure 7. Transfer receipt evidence

As shown in Figure 7. following the payment instructions, Victim A transferred Rp2,500,000 and submitted a transfer receipt through Instagram Direct Message. Examination of the recovered artifacts confirmed the existence of a digital transfer receipt attached to the communication thread. Metadata associated with the file demonstrated that the receipt was transmitted as part of the transaction process.

After receiving the transfer receipt, the suspect confirmed that the payment had been received and informed the victim that the top-up service was being processed. This finding is consistent with previous studies indicating that victims of online fraud often complete transactions based on trust

established through social media communication and promotional claims [4]. Extracted metadata confirms the payment receipt was transmitted directly within the transaction thread as proof of funds transfer.

Figure 8. Communication termination

As demonstrated in Figure 8, the parsed JSON logs reveal a distinct unilateral communication termination pattern. The timestamp metadata indicates that immediately after confirming payment, subsequent follow-up messages from the victim remained unacknowledged, followed by an account block. This behavioral artifact serves as crucial evidence establishing premeditated fraud intent.

However, subsequent examination revealed that the promised service was never delivered. Communication records showed that the suspect stopped responding after confirming receipt of payment. Multiple follow-up messages from the victim remained unanswered, indicating a unilateral termination of communication following successful payment.

This communication pattern strongly supports the hypothesis that the account was utilized as part of a fraudulent scheme involving Mobile Legends top-up services. This finding is consistent with common characteristics of social-media-based fraud cases reported in previous studies [24].

4.4. Evidence validation and integrity verification

To ensure the authenticity and reliability of the acquired evidence, several validation procedures were performed, including artifact comparison, metadata examination, and hash verification.

Suspect Archive	Victim Archive

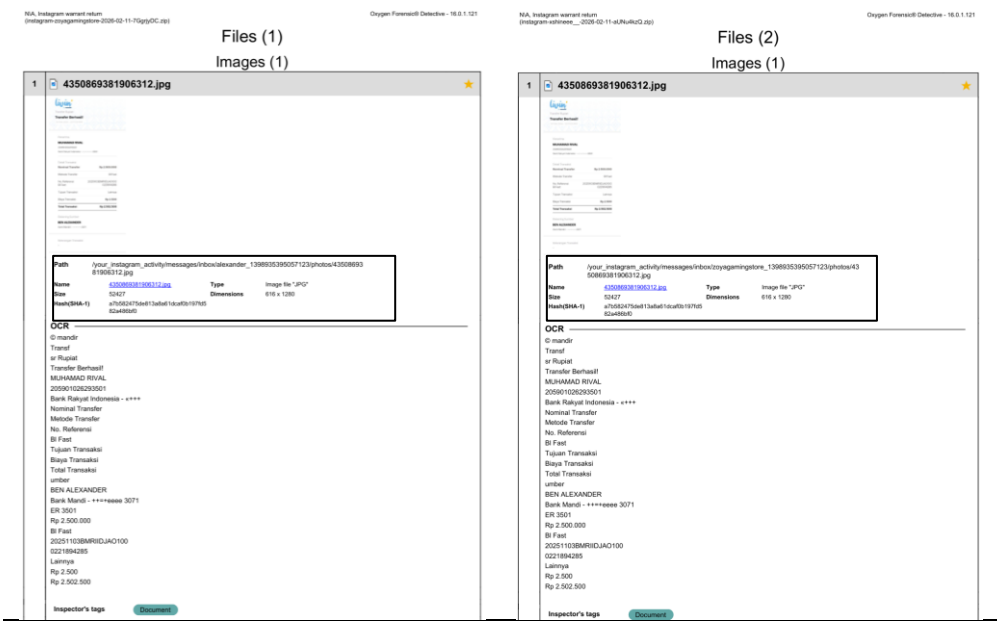

Figure 9. Comparison of transfer receipt artifacts

As shown in Figure 9. the consistency between both artifacts significantly strengthens the evidentiary value of the recovered transaction records. This finding indicates that the transaction evidence recovered from both archives originated from the same digital source. The comparison of digital artifacts from multiple sources is a common forensic validation technique used to establish evidence authenticity and support investigative findings [20].

Comparative analysis revealed that the transfer receipt recovered from the suspect's archive was identical to the receipt provided by Victim A. Both artifacts exhibited identical filenames, file sizes, image dimensions, SHA-1 hash values, and OCR extraction results. These findings indicate that both files originated from the same digital source and support the authenticity of the transaction evidence.

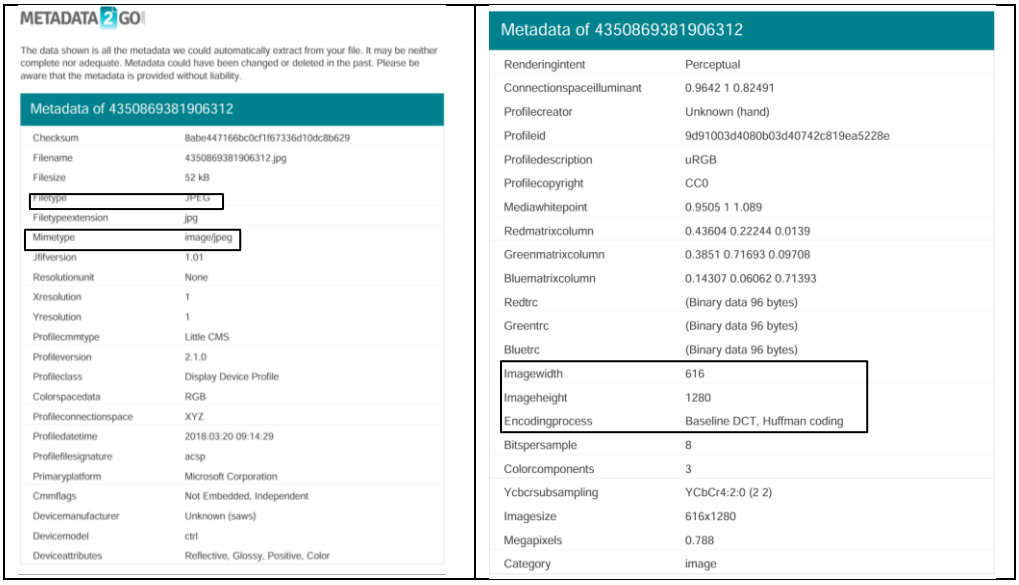

Figure 10. Metadata analysis result

Metadata analysis can be seen in Figure 10. was conducted using Metadata2Go. Examination results showed that the transfer receipt maintained normal JPEG characteristics, valid MIME type attributes, and standard image encoding parameters. Furthermore, no evidence of image editing software or metadata manipulation was detected. These findings indicate that the file maintained its

original characteristics and had not been modified. Therefore, the transfer receipt can be considered authentic and suitable for forensic analysis. Metadata examination provides important contextual information regarding the origin, characteristics, and integrity of digital evidence and is frequently utilized in forensic investigations [20].

Previous studies have demonstrated that metadata analysis can reveal information regarding file origin, creation history, device information, and potential modifications, making it an important component of digital forensic investigations [25].

The extracted metadata revealed that the transfer receipt image recovered from both archives possessed identical file attributes, including filename, file size, MIME type, dimensions, and timestamp information. The consistency of these metadata elements indicates that both parties retained the same digital artifact without modification.

The findings are consistent with previous forensic studies indicating that user activities and digital artifacts stored within social media platforms can be recovered and analyzed to support digital investigations and evidence reconstruction [26].

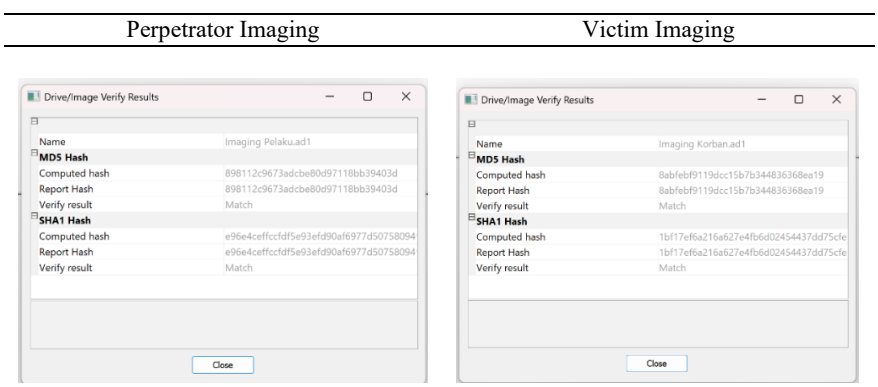

Figure 11. Hash verification result

As shown in Figure 11. to provide technical clarity on the hash matching process, FTK Imager calculates the mathematical checksum (Computed Hash) during verification and compares it against the initial hash recorded in the image file header (Report Hash). As summarized in Table 6, both MD5 and SHA-1 values returned a 100% match for both the suspect and victim archives.

Table 6. Forensic hash verification matrix (FTK imager)

Forensic Image Source	Algorithm	Computed Hash Value	Report Hash Value	Verification Result	Integrity Status
Suspect Archive	MD5	898112c9673adcbe80d97118bb39403d	898112c9673adcbe80d97118bb39403d	Match	Intact & Unaltered
	SHA-1	e96e4ceffccfdf5e93efd90af6977d5075809497	e96e4ceffccfdf5e93efd90af6977d5075809497	Match	Intact & Unaltered
Victim Archive	MD5	8abfebf9119dcc15b7b344836368ea19	8abfebf9119dcc15b7b344836368ea19	Match	Intact & Unaltered
	SHA-1	1bf17ef6a216a627e4fb6d02454437dd75cfe625	1bf17ef6a216a627e4fb6d02454437dd75cfe625	Match	Intact & Unaltered

Integrity verification was subsequently performed using FTK Imager through MD5 and SHA-1 hash calculations. Verification results demonstrated that the computed hash values matched the reported hash values for both the suspect's archive and the victim's archive. The matching hash values confirm that the digital evidence remained intact and unaltered throughout the acquisition and analysis processes.

Overall, the validation process demonstrated that the digital evidence obtained during the investigation was authentic, consistent, and forensically reliable. The recovered artifacts successfully reconstructed the fraud scenario, showing that victims completed payments for Mobile Legends top-up services that were never delivered. These findings demonstrate the effectiveness of the National Institute of Justice (NIJ) framework in supporting digital forensic investigations involving social media-based fraud cases.

Maintaining evidence integrity is an essential requirement in digital forensic investigations to ensure the admissibility and reliability of digital evidence [12]. Hash verification is widely used in digital forensic investigations to ensure that acquired evidence remains unchanged throughout the acquisition and examination processes [12].

5. Conclusion

This study successfully investigated a Mobile Legends top-up fraud case conducted through Instagram using the National Institute of Justice (NIJ) framework. By extracting 51 total digital artifacts from Instagram Download Your Information (DYI) JSON archives, the investigation successfully reconstructed the fraud pattern, established evidence continuity across 15 distinct victims, and verified 100% hash match integrity (MD5 and SHA-1).

The primary research contribution of this study lies in demonstrating the forensic admissibility and validity of Instagram's JSON archive data as primary digital evidence. Furthermore, it establishes a practical multi-tool methodology combining logical archive parsing, metadata validation, and dual-perspective cross-verification to uncover social media-based financial fraud.

However, this study has several limitations. The scope of the investigation was confined to a simulated environment focusing exclusively on Instagram's DYI archive structure and Android mobile artifacts. Consequently, the findings may not fully extend to live server-side memory acquisitions or other social media platforms with proprietary data formats. For future work, researchers are encouraged to expand this framework to live cloud forensics, explore automated JSON forensic parsers, and apply dual-perspective validation to multi-platform fraud schemes involving cross-app messaging.

Acknowledgements

The authors would like to express their sincere gratitude to the Department of Informatics, Faculty of Industrial Technology, Universitas Ahmad Dahlan, for providing academic support and research facilities. The authors also thank all individuals who contributed to this research through valuable discussions and technical assistance. This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Credit Authorship Contribution Statement

Auliana: Conceptualization, Methodology, Investigation, Data Curation, Software, Formal Analysis, Visualization, Writing – Original Draft. **Eko Aribowo:** Supervision, Validation, Methodology, Writing – Review & Editing, Project Administration.

Declaration of Competing Interests

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data Availability

The datasets generated and analyzed during the current study are not publicly available because they contain simulated digital forensic evidence and investigation artifacts but are available from the corresponding author on reasonable request.

Use of Artificial Intelligence

During the preparation of this manuscript, the authors used Generative Artificial Intelligence (AI) solely to improve language quality, grammar, and writing clarity. All scientific content, research design, data collection, forensic investigation, analysis, interpretation of results, and final conclusions were independently conducted, verified, and approved by the authors. The authors take full responsibility for the content of this manuscript.

References

[1] M. Barseli and V. Sriwahyuningsih, "Peran game online mobile legends sebagai pemicu turunnya motivasi belajar siswa," *J. Educ. J. Pendidik. Indones.*, vol. 9, no. 1, p. 164, Mar. 2023, doi: 10.29210/1202322743.

[2] M. Ambarwati, A. Rahman, and U. Sebelas Maret Surakarta, "Trash-Talking Pemain Mobile Legends: Bang Bang Mahasiswa FKIP UNS," *J. Ilmu Sos. dan Hum.*, vol. 5, 2022, [Online]. Available: https://jayapanguspress.penerbit.org/index.php/ganaya

[3] A. M. Fikri, "Kebijakan Hukum dalam Pemberantasan Pelaku Online Romance Fraud di Ruang Maya," *JCIC J. CIC Lemb. Ris. dan Konsult. Sos.*, vol. 6, no. 2, pp. 137–148, Sep. 2024, doi: 10.51486/jbo.v6i2.219.

[4] G. A. Pratama and A. S. Kusuma, "Kepercayaan di Internet: Studi Kasus pada Korban Layanan Top Up Game Online di Media Sosial," *J. Indones. Manaj. Inform. dan Komun.*, vol. 5, no. 3, pp. 2300–2312, 2024, doi: 10.35870/jimik.v5i3.892.

[5] Erni Yusnita Siregar and Muh Sulaiman, "PENGARUH KOMUNIKASI DAN KEBIJAKAN UU ITE TERHADAP TINDAK PIDANA PENIPUAN JUAL BELI BARANG ONLINE DI INSTAGRAM," vol. 3, 2021, Accessed: May 20, 2025. [Online]. Available: http://dx.doi.org/10.24014/je.v3i1.12592

[7] N. S. Ardi and S. Sukaris, "Analisis Resiko Penipuan Dalam Pembelian Online Di Instagram (Perspektif Konsumen)," *J. Mhs. Manaj.*, vol. 4, no. 02, p. 109, Apr. 2025, doi: 10.30587/mahasiswamanajemen.v4i02.9665.

[8] C. Hafiza, "Perlindungan Hukum Terhadap Korban Penipuan Belanja Online Melalui Aplikasi Shopee," *Sigma-Mu*, vol. 06, no. 05, p. 7, 2024.
Available: https://rama.unimal.ac.id/id/eprint/5234/

[9] H. S. Alawi, I. Riadi, and S. Sunardi, "Analisis Forensik Digital terhadap Kasus Penipuan pada E-Commerce Menggunakan Metode ACPO," *J. Inform. J. Pengemb. IT*, vol. 10, no. 3, pp. 789–801, 2025, doi: 10.30591/jpit.v10i3.8604.

[10] R. Jogja, "Generasi Muda Indonesia Rela Habiskan Uang Rp30 Triliun untuk Top Up Game Online." Accessed: Apr. 10, 2025. [Online].
Available:https://radarjogja.jawapos.com/entertainment/653172449/generasi-muda-indonesia-rela-habiskan-uang-rp30-triliun-untuk-top-up-game-online

[11] B. Pranawa, "Digital Forensik Sebagai Alat Bukti Terhadap ODGJ (Orang Dalam Gangguan Jiwa) Untuk Menentukan Pertanggungjawaban Pidana," *J. Bedah Huk.*, vol. 8, no. 1, pp. 16–29, Apr. 2024, doi: 10.36596/jbh.v8i1.1346.

[12] M. Safei, S. Dewi, and O. A. Johar, "Implementasi Pada Alat Bukti Jejak Digital Dalam Penegakan Hukum Tindak Pidana Penipuan Online," *Coll. Stud. J.*, vol. 8, no. 2, pp. 501–519, 2025, doi: 10.56301/csj.v8i2.2019.

[13] S. K. Saad, R. Umar, A. Fadlil, U. Ahmad, D. Jl, and S. H. Soepomo, "Analisis Forensik Aplikasi Dropbox pada Android menggunakan Metode NIJ pada Kasus Penyembunyian Berkas," *J. Sains Komput. Inform. (J-SAKTI*, vol. 4, no. September, p. 293, 2020. Available: https://www.researchgate.net/publication/395856910_Mobile_Forensic_Analysis_of_MiChat_Application_in_Human_Trafficking_Cases_using_National_Institute_of_Justice_Method

[14] S. Soni, Y. Fatma, and R. Anwar, "Akuisisi Bukti Digital Aplikasi Pesan Instan 'Bip' Menggunakan Metode National Institute of Justice (NIJ)," *J. CoSciTech (Computer Sci. Inf. Technol.*, vol. 3, no. 1, pp. 34–42, Jun. 2022, doi: 10.37859/coscitech.v3i1.3694.

[15] F. Anggraini, H. Herman, and A. Yudhana, "Akuisisi Bukti Digital Tiktok Berbasis Android Menggunakan Metode National Institute of Justice," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 10, no. 1, pp. 89–96, Mar. 2023, doi: 10.25126/jtiik.2023106416.

[16] Imam Riadi, Anton Yudhana, and Muhamad Caesar Febriansyah Putra, "Akuisisi Bukti Digital Pada Instagram MessengerBerbasis Android Menggunakan Metode NationalInstitute Of Justice

(NIJ)", Accessed: May 22, 2025. [Online]. Available: http://dx.doi.org/10.28932/jutisi.v4i2.769
[17] D. Karseno, B. Hendrik, and A. Kata Kunci, "Investigasi dan Analisis Pengembalian Pesan Whatsapp yang SudahTerhapus Menggunakan Metode National Institute of Justice (NIJ)," 2024. [Online]. Available: https://irje.org/index.php/irje
[18] D. Yuliana, T. Yuniati, and B. P. Zen, "ANALISIS FORENSIK TERHADAP KASUS CYBERBULLYING PADA INSTAGRAM DANWHATSAPP MENGGUNAKAN METODE NATIONAL INSTITUTE OF JUSTICE (NIJ)".
Available : https://ejournal.uin-suka.ac.id/saintek/cybersecurity/article/view/3734
[19] L. Julianti, "Web Forensics on Instagram Services using National Institute of Justice Method," vol. 185, no. 26, pp. 9–15, 2023.
Available: https://ijcaonline.org/archives/volume185/number26/julianti-2023-ijca-922957.pdf
[20] M. Riskiyadi, "INVESTIGASI FORENSIK TERHADAP BUKTI DIGITAL DALAM MENGUNGKAP CYBERCRIME," 2020.
Available: https://ejournal.uin-suka.ac.id/saintek/cybersecurity/article/view/2144
[21] M. Ali Diko Putra, A. Wirawan Muhammad, B. Parga Zen, R. Yunita Kisworini, and T. Rohayati, "Analisis Forensik Pada Instagram dan Tik Tok Dalam Mendapatkan Bukti Digital Dengan Menggunakan Metode NIST 800-86," *J. Sist. Inf. Galuh*, vol. 2, no. 1, pp. 44–54, 2024, doi: 10.25157/jsig.v2i1.3695.
[22] E. Dwi Ariyanti and D. Yusup, "IDENTIFIKASI BUKTI DIGITAL INSTAGRAM WEB DENGAN LIVE FORENSIC PADA KASUS PENIPUAN ONLINE SHOP," 2021. Available: https://ejournal.uin-suka.ac.id/saintek/cybersecurity/article/view/2436
[23] F. Nur, "Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana Penipuan OnlineDengan Modus Social Engineering," *Innov. J. Soc. Sci. Res.*, vol. 3, no. 4, pp. 342–355, 2025, [Online]. Available: https://j-innovative.org/index.php/Innovative
[24] M. Goa and H. Yusuf, "Analisis Penipuan Online Melalui Media Sosial Dalam Kasus Kejahatan Belanja Online di Wilayah Jawa Timur," *Media Huk. Indones.*, vol. 3, no. 3, 2025, [Online]. Available:
https://ojs.daarulhuda.or.id/index.php/MHI/article/view/2119%0Ahttps://ojs.daarulhuda.or.id/index.php/MHI/article/download/2119/2270
[25] M. C. Bunaen and R. P. Kristanto, "Pemanfaatan Forensically Beta Dan Metadata2go Dalam Analisis Keaslian Foto Digital," *Jupiter*, vol. 6, no. 2, pp. 221–230, 2025, doi: https://doi.org/10.53990/jupiter.v6i2.469
[26] R. Rahmansyah, "Perbandingan Hasil Investigasi Barang Bukti Digital Pada Aplikasi Facebook Dan Instagram Dengan Metode Nist," *Cyber Secur. dan Forensik Digit.*, vol. 4, no. 1, pp. 49–57, 2021, doi: 10.14421/csecurity.2021.4.1.2421.