

Improving Credibility of Digital Evidence Investigation in E-Commerce Fraud Cases using ISO/IEC 27037

Hanna Syahida Alawi¹, Imam Riadi², Sunardi³

¹Department of Informatics, Universitas Ahmad Dahlan, Yogyakarta, Indonesia

²Department of Information System, Universitas Ahmad Dahlan, Yogyakarta, Indonesia

³Department Electrical Engineering, Universitas Ahmad Dahlan, Yogyakarta, Indonesia

Article Info

Article history:

Received May 28, 2025

Revised Jul 14, 2025

Accepted Aug 19, 2025

Keywords:

TikTokShop fraud

Digital forensics

ISO/IEC 27037

Levenshtein

Image Compression

ABSTRACT

TikTokShop fraud is an emerging challenge in e-commerce investigations, demanding robust digital forensic approaches. This study tackles the complexities of investigating such fraud within the TikTokShop platform, focusing on the acquisition, preservation, and validation of multifaceted digital evidence, including screenshots, payment records, account data, videos, and communication logs. Adhering to ISO/IEC 27037 for evidence handling, Magnet and Oxygen forensic tools were used for systematic evidence acquisition. The analysis using Oxygen Forensic recovered 100% of relevant artifacts, which is slightly higher compared to Magnet Axiom, which recovered 38.46% of artifacts, although both tools were effective in retrieving critical artifacts such as image metadata, account information, and data transfers. Due to image compression by the TikTokShop application, discrepancies in hash values emerged, requiring supplementary validation. Optical Character Recognition (OCR) and Levenshtein distance algorithms quantified textual similarity within image-based evidence, while the Forensically platform enabled advanced image forensic analyses to detect potential tampering and authenticity. This rigorous, multi-layered forensic framework complements traditional hash verification by providing corroborative content-level authentication. Findings confirm that although hash inconsistencies arise from application-induced compression, integrating OCR, Levenshtein, and forensic image analysis enhances the reliability of digital evidence. The novelty of this research lies in its robust synergy of ISO/IEC 27037-compliant handling with advanced digital content verification, contributing to the advancement of digital forensic practices in complex social commerce fraud scenarios.

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



Corresponding Author:

Hanna Syahida Alawi,
Department of Informatics,
Universitas Ahmad Dahlan,
Jl. Ringroad Selatan, Kragilan, Tamanan, Banguntapan, Bantul, Special Region of Yogyakarta.
Email: 2407048009@webmail.uad.ac.id

1. INTRODUCTION

The advancement of e-commerce has significantly transformed the way digital transactions are conducted, providing unprecedented convenience and accessibility for both consumers and businesses

worldwide [1]. However, this progress has also resulted in a surge of fraudulent activities on online platforms, including payment fraud and identity misuse [2]. In Indonesia, the Ministry of Communication and Information recorded approximately 405,000 reports of online fraud between 2017 and 2024, with 13.1% of these cases involving e-commerce transactions in 2023 [3]. Similarly, the Indonesian Consumers Foundation (YLKI) reported that 13.1% of consumer complaints in 2023 were related to e-commerce transactions [4].

The rapid growth of TikTok, which surpassed Instagram with over one billion users in 2021 [5], has further complicated this issue. TikTok Shop, which integrates social media and e-commerce directly, enables users to easily discover and purchase products through the app [6]. However, this integration also creates new opportunities for cybercriminals to deceive consumers, such as by deleting chat messages and blocking victims' accounts to remove traces of digital evidence.

Digital forensics plays a crucial role in investigating and uncovering such crimes [7], [8]. In the context of TikTok Shop fraud, one of the primary challenges is verifying the authenticity of product images, which often serve as crucial evidence. Image verification is typically conducted using digital hash values. However, for compressed images commonly found on social media platforms hash values frequently change, rendering them unreliable for verification.

To address the limitations caused by hash value changes due to compression, this study adopts an alternative approach that leverages Optical Character Recognition (OCR) and the Levenshtein Distance algorithm to assess the textual similarity of payment proof images [9], [10], [11], [12], [13], [14], [15]. Visual verification is performed using the template matching technique provided by OpenCV [16], [17], [18], [19]. This integrated approach enables robust validation of both textual and visual content, thereby improving the reliability of forgery detection even when image formats have been altered [10].

Furthermore, this study utilizes Forensically Beta to conduct comprehensive visual analysis, particularly focusing on compressed product images as digital evidence [20]. The Error Level Analysis (ELA) feature within Forensically Beta highlights compression artifacts and inconsistencies in pixel structures, aiding in the detection of potential manipulation [21], [22], [23]. Meanwhile, the Level Sweep feature analyzes pixel intensity to identify areas that may have experienced abnormal compression or modifications [24], [25]. Emphasizing these features helps ensure the authenticity of compressed image evidence and its validity as legal evidence [26].

To maintain the integrity and reliability of digital evidence, this study adheres to the international standard ISO/IEC 27037:2012 [27], [28], [29], [30], [31], which has been proven effective in investigating non-volatile memory and acquiring digital evidence from IoT devices such as Smart CCTV [31]. Additionally, this study employs advanced forensic tools including Magnet AXIOM and Oxygen Forensic Detective, both of which have demonstrated capabilities in extracting data from social media applications such as TikTok, Instagram, and YouTube, as well as analyzing user data and activities [32], [33], [34], [35], [36]. The effectiveness of Oxygen Forensic Detective in extracting data from TikTok and similar applications has also been validated by previous studies [34], [37], [38], [39], [40].

The novelty of this study lies in integrating content-based text verification with visual analysis of compressed product images, which are generally challenging to authenticate especially within the context of e-commerce on TikTok Shop. This approach is expected to contribute significantly to enhancing the accuracy and legal validity of digital evidence, thereby supporting legal proceedings in court.

2. RESEARCH METHOD

This study uses the ISO/IEC 27037 method to conduct digital forensic analysis in fraud cases on TikTok Shop. This method consists of four main stages as illustrated in the Figure 1, which are identification, collection, acquisition, and preservation. The process aims to identify, obtain, and maintain the integrity of digital evidence related to transaction fraud on the e-commerce platform.



Figure 1. ISO/IEC 27037 Flow

2.1 Research Stage

Referring to Figure 1, the stages are as follows:

1. Identification.

The process of searching, recognizing, and documenting relevant digital evidence. Investigators identify devices that may contain evidence and determine the order of collection based on data volatility to minimize the risk of loss or damage.

2. Collection.

The process of gathering physical devices containing evidence and transferring them to a secure environment for further analysis. This includes documentation, packaging, and securing the devices before transportation.

3. Acquisition.

Creating a copy of data from devices containing evidence. The evidence copy must be verified to ensure authenticity and accuracy, and any changes during the process should be documented.

4. Preservation.

Maintaining the integrity and authenticity of evidence by storing it in a secure environment. This includes controlling access and maintaining the chain of custody to ensure the evidence remains intact and reliable.

This study examines fraud cases on TikTok Shop involving payments outside the platform's official system. The participants in this study are victims of fraud who were contacted to provide transaction data and communication history with the perpetrator. The collected data is analyzed using a digital forensic approach to identify patterns and evidence supporting the occurrence of fraud. All data and forensic procedures are well-documented to ensure the research results can be reproduced by other researchers.

2.2 Research Tools and Materials

This study utilizes several tools, as shown in Table 1.

Table 1. Research Tools

No	Device	Operating System	Status	Function
1	Oppo A57	Android Lollipop 5.0.1	<i>Rooted</i>	Research Object
2	Redmi 4X	Android Marshmallow 6.0.1	<i>Rooted</i>	Research Object
3	Laptop Lenovo Idepad e340	Windows 11 64 Bit	AMD RYZEN 3 8.00 GB RAM	Workstation for forensic analysis
4	USB Connector			Connects smartphone to workstation

Several software tools used to support the study are listed in Table 2. The software is categorized into test software, operating systems, forensic tools, and analysis tools.

Table 2. Supporting Software

No	Forensic Tool	Version	Function
1	TikTok Shop	2.17.351	Software test
2	Windows 11	11	Workstation operating system
3	Oxygen Forensic Detective	17.1.0.131	Forensic & analysis tool
4	Magnet Axiom	5.4.0.26185	Forensic & analysis tool
5	Android Debugging Bridge	1.4.3	Connects smartphone to workstation
6	Python	3.13	Analysis tool
7	Forensically Beta		Forensic & analysis tool

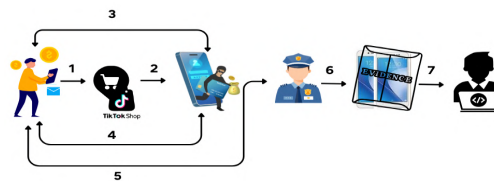


Figure 2. Research Scenario

2.3 Research Scenario

The following provides a detailed explanation of each step shown in Figure 2

1. Victim initiates a transaction
The victim initiates a purchase through TikTok Shop and communicates with the perpetrator via the chat feature to inquire about the product and available payment methods.
2. Perpetrator persuades the victim
The perpetrator convinces the victim to make the payment outside the official TikTok Shop system by offering a lower price.
3. Victim transfers money & sends proof
The victim follows the perpetrator's instructions, transfers the money directly, and sends the payment receipt through chat.
4. Perpetrator deletes traces
After receiving the money, the perpetrator blocks the victim and deletes the chat history to eliminate digital traces of the transaction.
5. Victim reports to the authorities
The victim reports the fraud to law enforcement authorities after realizing they have been scammed.
6. Authorities collect devices
Authorities collect the devices of both the victim and the perpetrator (if identified) as evidence for further investigation.
7. Digital forensic analysis
Digital forensic investigators analyze the collected devices using the ISO/IEC 27037 method, supported by tools such as Oxygen Forensic Detective and Magnet Axiom, to retrieve, examine, and verify digital evidence.

The decision to utilize a single, well-structured simulated fraud scenario in this study was a deliberate methodological choice to enable precise control, clarity of forensic process evaluation, and reproducibility of results. This focused design allowed for a systematic assessment of forensic

acquisition procedures, tool effectiveness, and validation techniques without the confounding variables typically present in uncontrolled case environments. Far from being a limitation, this approach establishes a robust proof-of-concept model that mirrors real-world social commerce fraud patterns and provides a reliable foundation for scalable forensic methodologies in future research.

2.4 Limitations of the Study

This study recognizes several methodological and practical limitations that define the scope of the research:

1. **Single Case Scenario**
The investigation focused on one simulated fraud case using two mobile devices. While this ensured procedural control, it may limit generalization to broader platforms or fraud patterns.
2. **Rooting Constraints**
Root access was performed ethically in a lab setting. However, in real-world cases, rooting may require legal authorization and is not always feasible on suspect or victim-owned devices.
3. **Focused Artifact Scope**
The qualitative analysis emphasized specific data types (e.g., deleted chats, image metadata). Future work should explore a wider variety of artifacts, including encrypted and app-specific logs.
4. **Image Validation Limitations**
OCR and Levenshtein Distance were effective in this context but may have reduced accuracy with altered or low-quality images.
5. **Tool Robustness and Failure Case**
Forensically Beta lacks formal metrics, making it prone to false positives under compression artifacts and limiting its reliability without additional verification.

Despite these limitations, the study provides a reliable and legally compliant forensic approach and serves as a foundation for future research on digital evidence in e-commerce fraud.

3. RESULTS AND DISCUSSION

This stage applies the digital forensic method in accordance with the ISO/IEC 27037 standard to the devices used in the research. Each step in this standard has a specific role that is interconnected and must be carried out sequentially to ensure the integrity and validity of the forensic investigation process.

3.1. Identification

At this stage, the investigator identifies devices and data that are potentially relevant as digital evidence in a TikTok Shop fraud case. The process continues by locating and collecting digital artifacts associated with fraudulent activities on the platform, as outlined in Table 3. The evidence obtained includes chat messages with the seller (including deleted content), transaction records, account credentials, multimedia files (such as images and videos), and application activity logs.

To enable access to system-level data, rooting was performed on two Android devices involved in this case: the Oppo A57 owned by the suspect, and the Redmi 4X belonging to the victim. This procedure allowed for the recovery of crucial artifacts such as deleted messages, internal logs, and protected application data that would not be accessible under standard user privileges. Rooting was conducted exclusively in a secure forensic laboratory environment and followed strict ethical protocols to ensure the integrity, authenticity, and admissibility of the acquired evidence.

In real-world digital forensic investigations, the use of rooting must comply with applicable legal frameworks and institutional policies, particularly when applied to devices belonging to victims or suspects. It is only considered valid when authorized by law, performed by certified forensic professionals, and fully documented. When these conditions are met, rooting is a legitimate and forensically sound technique, as supported by the principles of ISO/IEC 27037, which emphasize the controlled, reproducible, and legally justified acquisition of digital evidence.

This approach is consistent with recent forensic research [41], for instance, emphasized that although rooting may alter the system-level structure of a device, it remains an acceptable method in forensic acquisition provided that it is executed properly and thoroughly documented in accordance with forensic standards. In this study, all rooting procedures were implemented professionally and transparently, ensuring that the extracted evidence meets both technical and legal requirements.

The evidence identified during this phase contributes directly to the broader forensic analysis, supporting the reconstruction of fraud patterns, validation of user behavior, and identification of individuals involved in the fraudulent activity.

Table 3. Digital Evidence

Digital Evidence	Amount
Account Name	2
Picture	2
Video	1
Chat	8
Total	13

3.2. Collection

After the identification process, at the Collection stage, the device (smartphone) containing evidence related to fraud cases on Tik Tok Shop is secured by recording details such as brand, model, and serial number. The device is then packaged with anti-static and a unique identification mark. All processes are documented in the chain of custody to ensure the integrity of the evidence is maintained until the acquisition stage.



Figure 3. Detail Device

Figure 3 show the device is a smartphone in fairly good physical condition and the identified evidence in a powered-on state, then the collection priority is securing volatile data such as active memory and running applications before performing a full acquisition. The next step is to enable Airplane Mode to disconnect the device from the internet. The purpose of this mode is to prevent potential damage to the evidence on the smartphone, followed by activating the Developer Options

feature on the device. After that, the rooting process should be performed to gain privileged access to the device's file system, enabling the extraction of deeper system-level data, including hidden files and application data, before proceeding with the acquisition.

3.3. Acquisition

Proper citation Acquisition is performed by creating a bit-by-bit copy of the device data using Oxygen Forensic Detective and Magnet AXIOM to ensure the integrity of the evidence. The acquired data includes active files, deleted files, and related metadata. This process also includes verifying the acquisition results by comparing the hash value between the original data and the copy to ensure no changes or data manipulation have occurred.

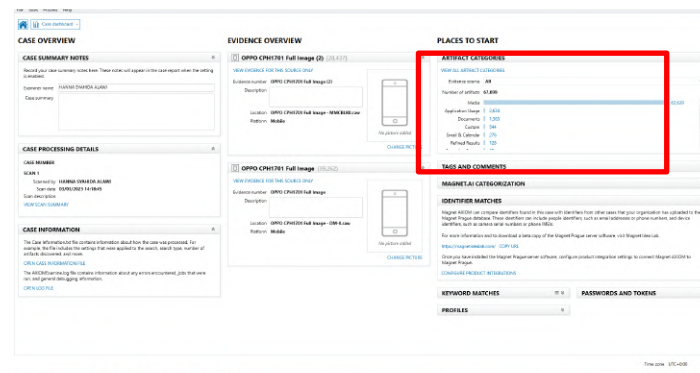


Figure 4. Acquisition Using Magnet AXIOM

Figure 4 shows the data acquisition results using the Magnet AXIOM tool with the logical method. This acquisition aims to extract all data stored on the OPPO CPH1701 device, including both existing data and deleted data. In the Evidence Overview section, it is shown that the device being analyzed is a mobile platform, and a total of 67,699 digital artifacts were successfully retrieved.

3.3.1 Acquisition Using Magnet AXIOM

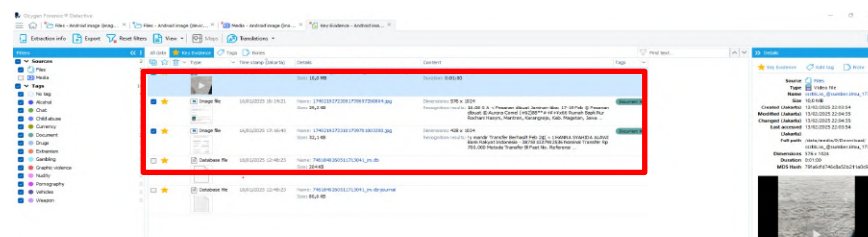


Figure 5. Video and Photos Identified Using Magnet AXIOM

Figure 5 show Magnet AXIOM successfully identified the presence of the TikTok application and recovered conversations deleted using the "Delete for Me" feature. However, artifacts related to TikTok Shop and conversations from blocked or deleted accounts were not found. This acquisition also successfully identified the accounts belonging to both the perpetrator and the victim, including important information such as usernames, account IDs, and profile links. In addition, a video suspected to have been sent by the perpetrator to convince the victim to conduct transactions outside the platform was also identified, along with two other pieces of evidence in the form of a transfer receipt photo and an order confirmation that were sent by the victim to the perpetrator.

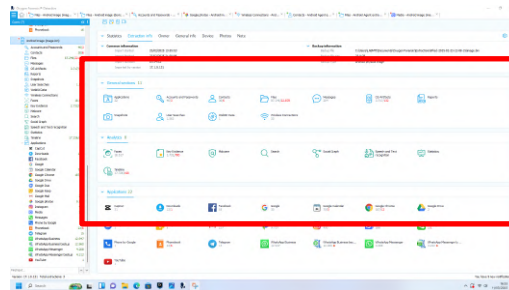


Figure 6. Acquisition Results using Oxygen Forensic Detective

Figure 6 shows the acquisition results using Oxygen Forensic Detective, which is capable of backing up data up to 23 GB; however, these results differ from those of Magnet AXIOM because Oxygen Forensic Detective was unable to detect the presence of the TikTok application, even though it was still installed on the device. Despite this, it was still able to extract the “db_im_contact” database, which was analyzed using SQLite with the “recovered data” option, revealing several deleted and active accounts that had communicated with the perpetrator.

3.3.2 Acquisition Using Magnet Oxygen



Figure 7. Chat Identified Using Oxygen Forensic Detective

Figure 7 shows the analysis results of a database named 7461840260511713041_im.db-journal, which contains evidence of deleted messages. This database was executed using SQLite with the “recovered data” option, allowing the recovery of deleted data. The display shows various message entries, including information such as the sender, message content, and message status. Additionally, the right panel contains metadata details for each message entry, including the sender ID, receiver ID, message type, and other related information. The displayed data indicates that deleted messages can still be recovered and analyzed for digital forensic purposes.

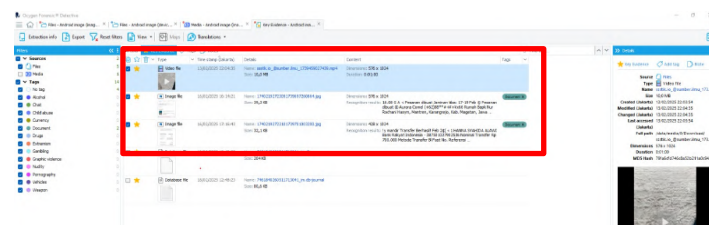


Figure 8. Video and Photos Identified Using Oxygen Forensic Detective

Figure 8 show Further analysis uncovered a video found in the Download folder, named ssstik.io_@sumber.ilmu_1739459027439.mp4, was used by the perpetrator to convince the victim of their legitimacy, with metadata such as file name, duration, and format supporting the forensic

investigation into fraudulent activity on TikTok Shop. Additionally, two relevant pieces of image evidence were found during the forensic investigation: a transfer receipt outside the platform, indicating payment outside the official TikTok Shop system, and a victim's order receipt containing order details made through the platform. These findings indicate that the perpetrator exploited communication outside the platform to commit the fraudulent act. Based on the analysis of the discovered image evidence, the images show a resemblance to the original image, although with a slight loss of quality resulting in blurriness. Comparison of the file size and hash values between the original image owned by the victim and the image received by the perpetrator revealed differences in hash values due to the reduced file size of the image received by the perpetrator. This reduction in size caused a change in hash value, as presented in Table 4, highlighting how compression can compromise the reliability of hash-based verification in digital forensic investigations.

In digital forensics, hash values serve as a critical indicator for verifying the integrity of digital evidence [42], [43]. However, in the context of social media and e-commerce platforms like TikTokShop, automatic compression that occurs when images are uploaded or transmitted often alters the binary structure of files, resulting in hash mismatches even when the visual content remains unchanged. This discrepancy can raise concerns regarding the admissibility or legal validity of the evidence, particularly when hash verification is used as the sole measure of authenticity.

To address this challenge, this study applies a comprehensive content-based validation approach by integrating four forensic techniques: Optical Character Recognition (OCR) to extract and compare text-based information, the Levenshtein algorithm to measure textual similarity, and visual forensic methods including Error Level Analysis (ELA) and Level Sweep to detect structural anomalies and potential image manipulation. This multi-faceted approach enables validation not only at the file level but also semantically, visually, and contextually. Technically, these methods complement each other and form a layered verification strategy. OCR detects text elements that are not verifiable through hash functions; Levenshtein quantifies textual similarity; and ELA and Level Sweep ensure there are no signs of visual tampering or compression-related distortions. This approach restores and reinforces the credibility of compressed evidence through comprehensive content validation.

From a legal standpoint, this methodology aligns with ISO/IEC 27037, which emphasizes the importance of procedural documentation, reproducibility, and multi-level analysis in establishing the credibility of digital evidence. Therefore, although hash values may change due to compression, as long as acquisition and validation are conducted transparently, properly documented, and with forensically sound methods, the evidence remains admissible in court. Consequently, the forensic strategy employed in this study is not merely a technical workaround, but a scientifically grounded and legally defensible framework for maintaining the integrity of digital evidence in dynamic environments.

Table 4. Comparison of File Sizes and Hash Values

Name Picture	Original Data		Evidence Using Oxygen		Evidence Using Magnet	
	Size	Hash	Size	Hash	Size	Hash
Proof of Order	235 KB (240.830 b)	ee3b324c5faf11236 493bfafb525a894	39,3 KB (40.335 b)	aa1c28fbaf63c60419 d18d4ddc878bb4	40335 b	aa1c28fbaf63c60419 d18d4ddc878bb4
Proof of payment	309 KB (316.423 b)	112b282975f5ed651 d13a9246f00056b	32,1 KB (32.892 b)	84b72dc44901dcc47 e9631ff75254a13	32892 b	84b72dc44901dcc47 e9631ff75254a13

The extraction process using the OCR feature in Oxygen Forensic Detective successfully identified order information, including the buyer's name, shipping address, contact number, item name, total price, and return policy. Despite the unclear condition of the evidence, the OCR feature was able to extract crucial information that supports the digital forensic investigation process.

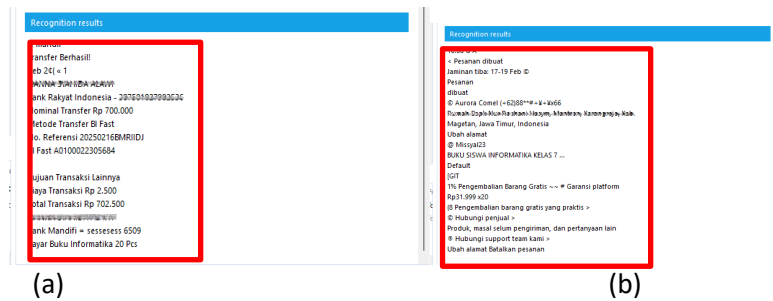


Figure 9. The OCR feature in Oxygen successfully detected the text within the images

Figure 9 show text extraction results using the OCR feature on Oxygen Forensic Detective demonstrate its capability to detect and recognize important information even under blurry image conditions. However, to determine the accuracy and similarity between the OCR-extracted text and the original image, further analysis and testing are required. The researcher used a Python source code that was developed to calculate the accuracy and similarity between the extracted text and the image through direct comparison using the Levenshtein calculation method and template matching

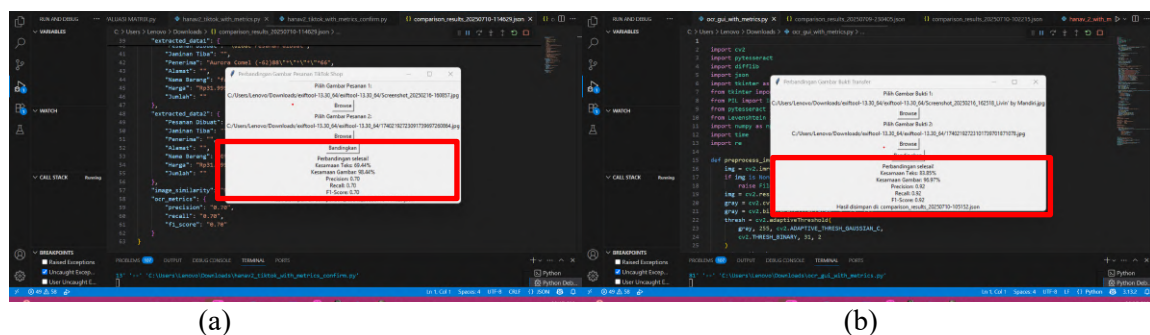


Figure 10. Result comparison using the Levenshtein calculation method and template matching.

Figure illustrates the interface of a digital forensic evaluation system designed to compare two types of digital evidence proof of payment and proof of order by integrating Optical Character Recognition (OCR) processing and textual similarity measurement using the Levenshtein distance algorithm, while incorporating formal evaluation metrics such as precision, recall, and F1-score to objectively assess OCR accuracy; in the first evaluation involving proof of payment, the system achieved a text similarity score of 83.85%, an image similarity score of 96.97%, and precision, recall, and F1-score values of 0.92, indicating a high level of accuracy in extracting critical transactional details, whereas in the second evaluation using screenshots of proof of order from TikTok Shop, the system recorded a text similarity of 69.44%, an image similarity of 98.44%, and precision, recall, and F1-score values of 0.70, demonstrating its capability to process and analyze digital artifacts with diverse visual formats; all evaluation results are automatically saved in JSON format to ensure the integrity, traceability, and admissibility of digital evidence in accordance with ISO/IEC 27037 standards, thereby supporting a legally valid and methodologically structured digital forensic investigation.

Table 5. Similarity comparison using python

Name Picture	Magnet Axiom		Oxygen Forensic Detective	
	Image Similarity	Text Similarity	Image Similarity	Text Similarity
Proof of Order	98.44%	69.44%	98.44%	69.44%
Proof of payment	96.97%	83.85%	96.97%	83.85%

The findings from Magnet AXIOM and Oxygen Forensic Detective, as presented in Table 5, show consistent accuracy in both text and image similarity measurements using the OCR and Levenshtein distance approach. While these methods effectively assess the degree of similarity between images and extracted text, they do not directly address the possibility of visual manipulation in the images. Therefore, to strengthen the verification that the images have not been tampered with, this research also utilizes additional tools such as Forensically Beta. Forensically Beta features include Error Level Analysis (ELA) and Level Sweep, which are crucial in detecting potential image manipulations. This comprehensive approach ensures that the images remain valid as evidence by not only measuring similarity but also confirming their authenticity through advanced forensic analysis.

Table 6. Comparison error level analysis and level sweep

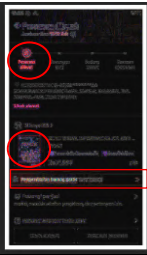
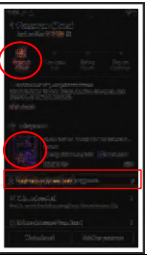
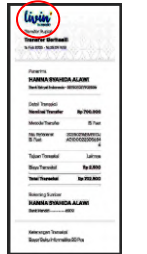
Original Image	Image Compression	ELA Original Image	ELA Image Compression	Level Sweep Original Image	Level Sweep Image Compression
					
					

Table 6 presents a comparative forensic analysis between the original and compressed versions of several images using two techniques from the Forensically Beta platform: Error Level Analysis (ELA) and Level Sweep. Each row displays a set of images analyzed across five stages: original image, compressed version, ELA on both, and Level Sweep visualizations.

The ELA results show localized anomalies (indicated with red circles) in the compressed images, particularly around text, icons, and structural elements. These anomalies involve variations in brightness and contrast caused by the automatic recompression process when images are uploaded to platforms such as TikTok Shop. This finding aligns with previous studies [20], which emphasize that

ELA is effective in detecting compression inconsistencies caused by basic editing or platform-induced re-encoding.

Meanwhile, the Level Sweep analysis provides a global visualization of color intensity distribution and internal image structure. Original images exhibit uniform color distribution and smooth tonal transitions, whereas compressed images show color banding, tonal irregularities in flat regions, and disturbances near object boundaries. These patterns are typical effects of lossy JPEG compression and do not indicate deliberate tampering. Prior studies [44], have also confirmed that Level Sweep is useful for identifying distributional anomalies caused by compression artifacts, even when no actual image manipulation occurs.

However, both techniques have limitations in terms of robustness and diagnostic precision. Neither ELA nor Level Sweep provides formal metrics such as error rates, confidence intervals, or quantitative scores. As a result, interpretation relies heavily on visual inspection and is susceptible to false positives, especially when artifacts are caused by aggressive compression rather than editing.

To overcome these limitations, this study integrates an additional validation layer through Optical Character Recognition (OCR) and content similarity measurement using the Levenshtein Distance. This multi-method approach is consistent with ISO/IEC 27037 principles, which emphasize the importance of reliability, reproducibility, and interpretability in digital evidence analysis.

Despite limitations in robustness and quantifiability, the combined use of ELA and Level Sweep offers valuable preliminary insights for investigation. Based on the results, although compression-induced visual distortions are present, there are no forensic indicators of tampering or object insertion. Therefore, the analyzed images can still be considered authentic and admissible as digital evidence.

3.4 Preservation

At this stage, the investigator maintains the integrity of the digital evidence by ensuring no changes are made to either the original data or the copy. The evidence is stored in a secure environment to prevent damage or modification. If unavoidable changes occur, all actions and reasons are thoroughly documented to maintain the validity of the evidence in legal proceedings.

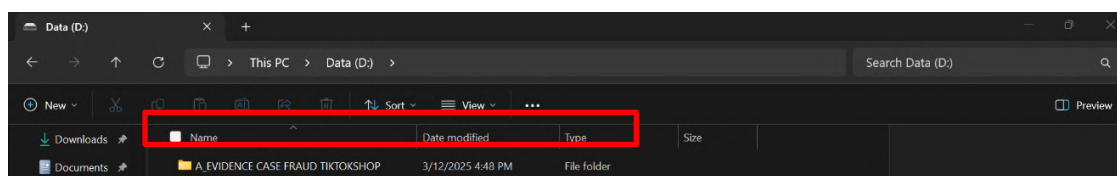


Figure 11. TikTok Shop Fraud Evidence Folder

Figure 11 shows a folder named "A_EVIDENCE CASE FRAUD TIKTOKSHOP" stored in the Data (D:) directory on a computer. This folder contains a copy of the evidence data related to a fraud case on TikTok Shop, which was acquired using digital forensic software. The copied data includes various digital artifacts, such as text messages, images, application usage history, and other data obtained from the OPPO CPH1701 device during the investigation process. Storing the copied data in this directory aims to maintain the authenticity and integrity of the evidence to support further analysis and examination in accordance with digital forensic standards. This practice is essential to maintain the validity of the evidence in legal proceedings. By preserving both metadata and hash values of the acquired files, investigators ensure that the evidence remains unchanged and verifiable. Additionally, a proper chain of custody is upheld to demonstrate the credibility and reliability of the digital evidence throughout the forensic process.

This research was conducted based on the four stages outlined in the ISO/IEC 27037 standard, using two digital forensic software tools: Magnet AXIOM and Oxygen Forensic Detective. The purpose of this testing was to evaluate the effectiveness of each software in identifying and acquiring digital evidence from the analyzed device. The analysis results revealed differences in data acquisition capabilities, particularly in extracting text message data (chat). A detailed comparison of the acquisition results from both software tools is presented in Table 7, which includes the quantity and type of digital evidence successfully identified by each tool.

Table 7. Comparison of Digital Evidence Acquisition Results Between Magnet AXIOM and Oxygen Forensic Detective

Digital Evidence	Amount	Magnet Axiom	Oxygen Forensic Detective
Account Name	2	Found	Found
Picture	2	Found	Found
Video	1	Found	Found
Chat	8	Not Found	Found
Total	13	5	13

To calculate the comparison of data acquisition results between Magnet AXIOM and Oxygen Forensic Detective on table 7, we can use the accuracy formula as follows:

$$Par = P \left(\frac{\sum ar0}{\sum arT} \right) \times 100\% \quad (1)$$

Par = Accuracy index of the forensic tool used.

$\sum ar0$ = Number of material parameters detected by the forensic tool.

$\sum arT$ = Total number of material parameters used in the analysis

$$Par \text{ Magnet Axiom} = \left(\frac{5}{13} \right) \times 100\% = 38.46\%$$

$$Par \text{ Oxygen} = \left(\frac{13}{13} \right) \times 100\% = 100\%$$

This formula is used to determine the accuracy level of forensic tools by comparing the number of successfully identified parameters with the total parameters used in the analysis process. The calculation result is expressed as a percentage, representing the effectiveness of the forensic tool in detecting relevant evidence or materials during the digital investigation [8].

In addition to the quantitative comparison of the number of digital artifacts retrieved by Magnet AXIOM and Oxygen Forensic Detective, this study also incorporates a qualitative evaluation to assess the forensic relevance of the extracted artifacts. Magnet AXIOM demonstrated broader coverage in acquiring general data such as system logs and application metadata, whereas Oxygen Forensic Detective proved more effective in recovering artifacts with direct relevance to the fraud investigation such as deleted chat messages and metadata embedded in image files linked to fraudulent activity.

The chat messages recovered by Oxygen revealed persuasive communication strategies used by the suspect, including attempts to redirect the victim to off-platform transactions and apply verbal pressure consistent with manipulative tactics. Metadata associated with transactional images, including timestamps, geolocation data, and source application identifiers, added critical authenticity and temporal context that supported reconstruction of the fraud timeline.

While Oxygen did not detect the TikTok Shop application interface in its entirety, its ability to parse database files and extract deleted entries played a key role in uncovering hidden interactions

between the suspect and the victim. This demonstrates that forensic acquisition should not rely solely on interface-level data but also on structured internal data artifacts with high evidentiary value.

These findings reinforce the notion that forensic tool effectiveness should not be measured solely by the quantity of artifacts recovered. Instead, greater emphasis must be placed on the contextual depth, legal admissibility, and narrative relevance of the evidence. Therefore, a comprehensive forensic analysis requires not only quantitative outcomes but also a structured qualitative assessment to ensure technically valid and legally defensible conclusions.

4. CONCLUSION

This study successfully verified the authenticity of digital data on the TikTok Shop platform, in line with the objectives outlined in the Introduction chapter, by demonstrating that digital forensic methods can identify differences in artifacts between original files and those that have undergone compression. The analysis using Oxygen Forensic recovered 100% of relevant artifacts, which is slightly higher compared to Magnet Axion, which recovered 38.46% of artifacts, although both tools were effective in retrieving critical artifacts such as image metadata, account information, and data transfers. The Error Level Analysis (ELA) and Level Sweep methods revealed compression variations without any significant content manipulation, while the application of Levenshtein Distance revealed a high degree of text similarity between the original and compressed versions, and Template Matching verified that no substantial differences were present in critical visual areas. These findings suggest that even after compression, the data remains suitable as valid evidence in digital forensic investigations, and they provide a foundation for the future development of more precise digital manipulation detection tools.

ACKNOWLEDGEMENTS

The author would like to express sincere gratitude to the academic advisors for their guidance, direction, and support throughout the research process. Appreciation is also extended to Ahmad Dahlan University for the facilities and support provided during the execution of this research. Furthermore, the author acknowledges the assistance from all parties who contributed to language refinement, writing guidance, and the proofreading process of this article. Special thanks are given to the experts and colleagues who provided valuable insights and technical support during the research process. Lastly, the author would like to express heartfelt gratitude for the continuous encouragement and support from family and friends throughout this research journey.

REFERENCES

- [1] S. Saeed, "A Customer-Centric View of E-Commerce Security and Privacy," *Appl. Sci.*, vol. 13, no. 2, 2023, doi: 10.3390/app13021020.
- [2] Sucipto, "Kemenkominfo Catat 405.000 Laporan Penipuan Transaksi Online Sepanjang 2017-2024," *Sindonews*, 2024. [Online]. Available: <https://nasional.sindonews.com/read/1419745/13/kemenkominfo-catat-405000-laporan-penipuan-transaksi-online-sepanjang-2017-2024-1721524077/>
- [3] H. S. Mikayla, A. Kusyanti, and P. H. Trisnawan, "Analisis Forensik Digital untuk Investigasi Kasus Cyberbullying pada Media Sosial Tiktok," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 10, no. 7, pp. 1571–1582, 2023, doi: 10.25126/jtiik.1078017.
- [4] D. Rachmawati, "YLKI Ungkap Pengaduan Konsumen Terbanyak di Sektor E-commerce," *Bisnis.com*, 2024. [Online]. Available: <https://ekonomi.bisnis.com/read/20240123/12/1734816/ylki-ungkap-pengaduan-konsumen-terbanyak-di-sektor-e-commerce>
- [5] M. Boeker, *An Empirical Investigation of Personalization Factors on TikTok*, vol. 1, no. 1. Association for Computing Machinery, 2022. doi: 10.1145/3485447.3512102.

- [6] Z. R. F. Nur, I. N. N. Rabbiana, T. Diba, and F. Fitroh, "TikTok Shop: Unveiling the Evolution from Social Media to Social Commerce and its Computational Impact on Digital Marketing," *J. Comput. Sci. Eng.*, vol. 4, no. 2, pp. 88–96, 2023, doi: 10.36596/jcse.v4i2.512.
- [7] I. Riadi and R. Umar, "Mobile Forensics in Human Trafficking Investigation Services U sing Mobile Laboratory," *JUITA J. Inform.*, vol. 13, no. 1, pp. 1–10, 2025, [Online]. Available: <https://doi.org/10.30595/juita.v13i1.24060>
- [8] 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, doi: 10.15294/sji.v8i1.26744.
- [9] A. Birr, K. Susanto, N. Muliadi, and B. Nugroho, "Comparison of String Similarity Algorithm in post- processing OCR," *J. Appl. Intell. Syst. (e-ISSN)*, vol. 8, no. 1, pp. 25–32, 2023.
- [10] R. Febriana and A. Luthfi, "Comparative Study of Cloud Forensic Investigation Using ADAM And NIST 800-86 Methods in Private Cloud Computing," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 5, no. 158, pp. 1–10, 2023.
- [11] S. Faizullah, M. S. Ayub, T. Alghamdi, T. S. Ali, M. A. Khan, and E. Nabil, "Revolutionizing Historical Document Digitization: LSTM-Enhanced OCR for Arabic Handwritten Manuscripts," *Int. J. Adv. Comput. Sci. Appl.*, vol. 15, no. 10, pp. 1185–1194, 2024, doi: DOI: 10.14569/IJACSA.2024.01510120 PDF.
- [12] P. Wang and C. Yao, "Levenshtein OCR," *arXiv*, vol. 2, no. 1, pp. 1–17, 2023.
- [13] Y. Chen, "Adopting Glyph Embedding for Improved Correction," *arXiv*, vol. 1, no. 1, pp. 1–5, 2023.
- [14] M. Dias and C. T. Lopes, "Optimization of Image Processing Algorithms for Character Recognition in Cultural Typewritten Documents," *arXiv*, vol. 1, no. 1, pp. 1–25, 2023, doi: 10.1145/3606705.
- [15] A. Beshirov, P. Nakov, M. Dobрева, D. Dimitrov, M. Hardalov, and I. Koychev, "Post-ocr text correction for Bulgarian historical documents," *Int. J. Digit. Libr.*, vol. 26, no. 1, pp. 1–11, 2025, doi: 10.1007/s00799-025-00415-x.
- [16] V. Quantized, N. Neighbour, A. Gupta, and I. Sintorn, "Efficient High-Resolution Template Matching with," *arXiv*, vol. 3, no. 1, pp. 1–43, 2023.
- [17] C. V. Media, "Learning Accurate Template Matching with Differentiable Coarse-to-Fine Correspondence Refinement ©," *Springer*, vol. 1, no. 1, pp. 1–21, 2023.
- [18] A. Hristov and D. Dimov, "Self-Supervised Foundation Model for Template Matching," *MDPI*, vol. 9, no. 1, pp. 3–25, 2025.
- [19] M. Annaby and Y. Fouda, "Fast template matching and object detection techniques using ϕ - correlation and binary circuits," *Springer*, vol. 83, no. 1, pp. 6469–6496, 2024.
- [20] R. Gorle, "Enhanced Image Tampering Detection using Error Level Analysis and a CNN," *Eng. Appl. Sci. Research*, vol. 15, no. 1, pp. 19683–19689, 2025.
- [21] W. P. Sari and H. Fahmi, "The effect of error level analysis on the image forgery detection using deep learning," *Kinetik*, vol. 4, no. 3, pp. 187–193, 2021.
- [22] S. Chourasiya and G. G. Vishwavidyalaya, "International Journal of Forensic Sciences," *Int. J. Forensic Sci.*, vol. 8, no. January 2023, pp. 1–10, 2024, doi: 10.23880/ijfsc-16000292.
- [23] H. Fayyad-kazan, E. Saba, H. J. Hejase, and A. El Dirani, "JPEG Steganography : Hiding in Plain Sight," *Int. J. Forensic Sci.*, vol. 6, no. 1, pp. 1–11, 2021, doi: 10.23880/ijfsc-16000223.
- [24] S. Chourasiya, V. Patel, and R. Pandey, "Forensic Document Examination Using Image Processing Tools," *Int. J. Forensic Res.*, vol. 8, no. 1, pp. 1–9, 2023, doi: 10.23880/ijfsc-16000292.
- [25] O. Maulidya and I. Riadi, "Image Forensics to Detect Image Authenticity using Error Level Analysis and Noise Analysis Methods," vol. 185, no. 28, pp. 6–11, 2023.
- [26] A. Dan, B. Matching, I. Sudianto, and N. Anwar, "Analisa Forensik Citra Menggunakan Metode Error Level," *J. Sarj. Tek. Inform.*, vol. 11, no. 1, pp. 40–48, 2023.

- [27] *International Standard ISO / IEC Information technology — Security techniques — Guidelines for identification , collection , acquisition , and preservation of digital evidence*, First Edit., vol. 2012. ISO Copyright Office, 2012. [Online]. Available: <https://www.iso.org/standard/44381.html>
- [28] A. Wickramasekara, F. Breiting, and M. Scanlon, “Exploring the potential of large language models for improving digital forensic investigation efficiency,” *Forensic Sci. Int. Digit. Investig.*, vol. 52, no. February, p. 301859, 2025, doi: 10.1016/j.fsidi.2024.301859.
- [29] K. A. Z. Ariffin and F. H. Ahmad, “Indicators for maturity and readiness for revolution 4.0,” *Comput. Secur.*, vol. 105, pp. 1–25, 2021, [Online]. Available: <https://doi.org/10.1016/j.cose.2021.102237>
- [30] D. Stabili, F. Valgimigli, and M. Marchetti, “I know where you have been last summer : Extracting privacy-sensitive information via forensic analysis of the Mercedes-Benz NTG5 * 2 infotainment system,” *Forensic Sci. Int. Digit. Investig.*, vol. 53, no. March, p. 301909, 2025, doi: 10.1016/j.fsidi.2025.301909.
- [31] A. Rizdqi and R. S. D. H. Panji, “Digital Forensic Investigation for Non-Volatile Memory Architecture by Digital Forensic Investigation for Non-Volatile Memory Architecture by Hybrid Evaluation Based on ISO / IEC 27037 : 2012 and NIST SP800-86 Framework,” *IT J. Res. Dev.*, vol. 6, no. February, pp. 162–168, 2022, doi: 10.25299/itjrd.2022.8968.
- [32] I. Riadi, H. Herman, and I. A. Rafiq, “Mobile Forensic Investigation of Fake News Cases on Instagram Applications with Digital Forensics Research Workshop Framework,” *Int. J. Artif. Intell. Res.*, vol. 6, no. 2, 2022, doi: 10.29099/ijair.v6i2.311.
- [33] F. Anggraini, H. 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, p. 1117, 2022, doi: 10.30865/jurikom.v9i4.4738.
- [34] T. Sutikno, “Mobile forensics tools and techniques for digital crime investigation: a comprehensive review,” *Int. J. Informatics Commun. Technol.*, vol. 13, no. 2, pp. 321–332, 2024, doi: 10.11591/ijict.v13i2.pp321-332.
- [35] H. Imanuel Gilbert Rian, Mailangkay., Elia, Zakharia., Abdul, “Komparasi Analisis Bukti Digital Tiktok Lite Menggunakan Metode National Institute of Justice,” *J. Sains Komput. Inform. (J-SAKTI)*, vol. 6, no. 2, pp. 661–670, 2022.
- [36] I. Riadi, Herman, and N. H. Siregar, “Mobile Forensic Analysis of Signal Messenger Application on Android using Digital Forensic Research Workshop (DFRWS) Framework,” *Ing. des Syst. d'Information*, vol. 27, no. 6, pp. 903–913, 2022, doi: 10.18280/ISI.270606.
- [37] G. R. Panigrahi, N. K. Barpanda, and P. K. Sethy, “Navigating the cyber forensics landscape a review of recent innovations,” *Int. J. Informatics Commun. Technol.*, vol. 13, no. 1, pp. 27–33, 2024, doi: 10.11591/ijict.v13i1.pp27-33.
- [38] E. al. Varshapriya N Jyotinagar, “A Conceptual Cloud Forensic Investigation Process Model for Software as a Service(SaaS) Applications,” *Int. J. Recent Innov. Trends Comput. Commun.*, vol. 11, no. 10, pp. 838–844, 2023, doi: 10.17762/ijritcc.v11i10.8600.
- [39] I. Riadi, H. Herman, and N. H. Siregar, “Mobile Forensic of Vaccine Hoaxes on Signal Messenger using DFRWS Framework,” *MATRIK J. Manajemen, Tek. Inform. dan Rekayasa Komput.*, vol. 21, no. 3, pp. 489–502, 2022, doi: 10.30812/matrik.v21i3.1620.
- [40] T. Ruslan, I. Riadi, and S. Sunardi, “Analisis Forensik Digital Pada Whatsapp Dan Facebook Menggunakan Metode NIST,” *J. Fasilkom*, vol. 13, no. 02, pp. 286–292, 2023, doi: 10.37859/jf.v13i02.5540.
- [41] N. Yalçın and T. Yıldırım, “Logical Image Acquisition and Analysis of Android Smartphones,” *J. Comput. Commun.*, vol. 12, no. 1, pp. 139–152, 2024, doi: 10.4236/jcc.2024.124011.
- [42] B. Guttman, D. R. White, and D. R. White, “NIST Interagency Report NIST IR 8387 Digital International Journal of Advances in Data and Information Systems, Vol. 6, No. 2, August 2025, pp. 479–495

- Evidence Preservation Considerations for Evidence Handlers NIST IR 8387,” *NIST Interag. Rep. NIST IR 8387 Digit.*, vol. 1, no. 1, pp. 1–22, 2022, doi: <https://doi.org/10.6028/NIST.IR.8387>.
- [43] A. A. Thakar, P. B. V Patel, and K. Kumar, “An Empirical Study Illustrating Effects on Hash Value Changes in Forensic Evidence Appreciation,” *Int. J. Sci. Res.*, vol. 10, no. 4, pp. 1356–1358, 2021, doi: 10.21275/SR21501151311.
- [44] R. Joshi, G. Abhishek, K. Nandan, and G. Pandharinath, “Forged Image Detection using SOTA Image Classification Deep Learning Methods For Image Forensics With Error Level Analysis,” *arXiv*, vol. 1, no. 1, pp. 1–8, 2022.