Mobile Forensic Investigation of E-Commerce Fraud Using DFRWS Method and Perceptual Hashing

Rizal Prambudi[1*], Imam Riadi[2], Murinto[3]

[1,3] *Department of Informatics, Universitas Ahmad Dahlan, Yogyakarta, Indonesia*
[2]*Department of Information System, Universitas Ahmad Dahlan, Yogyakarta, Indonesia*

*corr-author: 2407048005@webmail.uad.ac.id

Abstract - Social media platforms have enabled real-time communication and broad user interaction, but they are often exploited for cybercrime. One such vulnerable medium is e-commerce applications, which facilitate transactions and store sensitive user data. This study investigates digital evidence in a simulated fraud case involving an e-commerce application by applying mobile forensic techniques guided by the Digital Forensic Research Workshop framework. The investigation focused on recovering user accounts, text messages, images, and videos from an Android smartphone. Two forensic tools Oxygen Forensic Detective and MOBILedit Forensic Express were used for data extraction and analysis. To improve the reliability of visual evidence, the study incorporated perceptual hashing and wavelet hashing techniques to validate compressed image files. The results showed that Oxygen Forensic Detective recovered 71.4% of digital evidence, while MOBILedit achieved 57%. Although both tools successfully recovered multimedia files, Oxygen performed better in extracting text messages. These findings demonstrate the effectiveness of mobile forensic methods in identifying and validating digital evidence in e-commerce fraud cases. Moreover, integrating the DFRWS methodology with perceptual hashing significantly improves the interpretation of manipulated or compressed images, thus enhancing the evidentiary value for legal proceedings.

Keywords: Mobile device analysis; e-commerce; DFRWS; perceptual hash; digital criminal activity.

I. INTRODUCTION

The rapid advancement of Industry 4.0 has accelerated digital transformation across multiple sectors, particularly in mobile technology. The widespread adoption of smartphones enables individuals to communicate, access information, exchange data, and conduct digital transactions such as online shopping. In Indonesia, the number of e-commerce users reached 58.63 million in 2023 and is projected to rise to 99.1 million by 2029 [1]. Shopee, one of the most frequently visited platforms, recorded 131.3 million visits in the second quarter of 2022 [2]. This significant growth in digital transactions has been accompanied by an increase in mobile-based cybercrime. Therefore, maintaining the integrity, authenticity, and traceability of evidentiary data retrieved from mobile devices is critical in digital forensic investigations, especially when handling dynamic, compressed, or altered artifacts as found in previous analyses of mobile messaging applications such as Signal [3] and MiChat [4].

Previous research applied the Association of Chief Police Officers framework with forensic tools such as Oxygen Forensic Detective and MOBILedit Forensic Express to extract digital artifacts from mobile devices [5]. Although both tools effectively recover application level data, challenges persist in validating image artifacts automatically compressed by e-commerce platforms. Compression processes may modify cryptographic hash values and weaken evidential integrity [6,7]. Numerous investigations have examined messaging applications using ACPO [8] and DFRWS [9,10], yet limited research focus on forensic analysis of mobile based e-commerce applications. Recent findings highlight the need to examine metadata structures, evaluate compression impacts, and enhance image validation mechanisms [11,12,13]. Cryptographic hashing algorithms such as SHA-1 and SHA-256 remain insufficient for detecting post-compression or format transformation changes [14].

Despite the availability of standardized forensic frameworks and professional tools, current mobile forensic investigations of e-commerce fraud lack a formal quantitative mechanism for validating compressed visual evidence in a legally defensible manner. Existing workflows emphasize procedural stages of evidence handling while providing limited analytical support for assessing the integrity and authenticity of compressed image artifacts. This limitation is particularly critical in e-commerce environments, where automated platform-level compression and content transformation are routinely applied.

To address these challenges, this research employs Oxygen Forensic Detective and MOBILedit Forensic Express for data acquisition due to their advanced capabilities, including full-disk imaging, encrypted data recovery, and deep SQLite database parsing in Android environments [15]. These tools offer advantages over general purpose forensic software such as Autopsy or FTK Imager, which are less optimized for mobile ecosystems or cloud based data [16]. Both support automatic hash generation and structured reporting, essential for maintaining traceability and accountability in e-commerce fraud investigations involving hybrid application web environments and session-based authentication [17].

This research adopts the Digital Forensic Research Workshop (DFRWS) framework, which consists of six structured stages identification, acquisition, preservation, examination, analysis, and presentation [18]. Unlike the ACPO framework, which primarily emphasizes procedural compliance and chain of custody, the DFRWS framework provides greater flexibility for analytical integration during the examination and analysis phases. In this context, perceptual hashing techniques namely aHash, dHash, pHash, and wHash are incorporated to validate compressed or transformed image evidence. These algorithms tolerate minor visual modifications while preserving content-based similarity, enabling detection of visually equivalent or manipulated images under compression [19,20]. This capability is highly relevant in mobile forensic contexts where image compression and data transformation frequently occur [21].

Based on these considerations, this research is founded on analytically testable assumptions that content-based perceptual hashing provides higher accuracy and robustness for validating compressed mobile image evidence when conventional cryptographic hashing becomes ineffective, and that physical forensic acquisition using Oxygen Forensic Detective yields a higher recovery rate of relevant digital artifacts compared to MOBILedit Forensic Express. These assumptions constitute the analytical basis for a quantitative comparison of forensic tools and image validation techniques employed in this research.

Accordingly, this research develops a content-based forensic validation model that integrates perceptual hashing into the DFRWS framework to extend its analytical capacity. The research evaluates four perceptual hashing algorithms aHash, dHash, pHash, and wHash in validating image evidence extracted from mobile e-commerce applications and compares their performance against conventional cryptographic hashing methods such as MD5 and SHA-256. Methodologically, this approach transforms DFRWS from a procedural workflow into a quantitative analytical framework capable of measuring forensic accuracy. Technically, it establishes perceptual hashing as a reliable mechanism for preserving evidentiary integrity and supporting the legal admissibility of mobile forensic artifacts under recognized digital investigation standards.

II. METHOD

This research conducted a mobile digital forensic investigation at the Digital Forensic Laboratory of Universitas Ahmad Dahlan by simulating an e-commerce fraud case. The DFRWS framework was adopted for its structured and flexible process, especially in handling digital transaction artifacts. Unlike the ACPO framework, which emphasizes procedural and legal compliance, DFRWS supports advanced technical analysis, including for compressed or modified image artifacts. Forensic tools such as Oxygen Forensic Detective and MOBILedit Forensic Express were used to acquire encrypted and hidden data directly from mobile devices. After acquisition, the image artifacts were validated using perceptual hashing which are effective in detecting visual similarity despite changes in size, format, or compression. The DFRWS process ensures that all forensic procedures comply with legal standards, making the results admissible in court. The methodology of this research involved several stages, summarized as follows:

This research continues previous research [5] by collecting relevant data from journals, articles, and academic sources related to digital forensics, mobile e-commerce fraud, and image validation. The literature review was conducted using platforms such as Google Scholar, ResearchGate, and ScienceDirect to support the development of the forensic framework and hashing validation approach.

A. Case Simulation

This This stage involved the implementation of a fraud scenario within a mobile e-commerce application, using the perpetrator's smartphone as the primary source of digital evidence. In this simulation, the suspected fraudster was apprehended, and their Android device was seized for forensic examination. The details of the scenario are depicted in Fig. 1.

Fig. 1 Case simulation

Fig. 1 illustrates a case in which the perpetrator listed a product for sale on an e-commerce platform, and the victim completed a purchase from the perpetrator's storefront. Upon receiving the item, the victim discovered that the delivered product did not match the advertised specifications. The incident was subsequently reported to law enforcement, who uncovered that the perpetrator had deleted transaction records in an attempt to destroy potential evidence. In response to the report, investigators secured a Samsung SM-G532G smartphone, which was identified as the key source of digital evidence.

B. Forensic Analysis

This research focuses on four primary variables: user accounts, images, videos, and text messages. These variables were analyzed to uncover digital evidence related to an e-commerce fraud case using Oxygen Forensic Detective and MOBILedit Forensic Express. The investigation followed the DFRWS framework, enhanced with perceptual hashing based validation, as illustrated in Fig. 2.

Explanation of Fig. 2. Perceptual hashing–enhanced DFRWS Process Stages:

1) Identification: The initial stage involves identifying the digital evidence source, which in this case is the Android smartphone belonging to the suspected fraudster. The device was selected based on indications of illicit activity conducted via the Shopee application.

2) Preservation: This stage ensures data integrity by performing forensic imaging of the original device onto separate storage media. The original device is not used during analysis to avoid accidental modifications, thus preserving the evidentiary value.

3) Collection: Relevant data were extracted using forensic tools MOBILedit and Oxygen Forensic. The collected artifacts included SQLite databases, product images, transaction history, and cache files from the Shopee mobile application. All extracted data were securely backed up for further examination.

4) Examination: During this stage, the extracted data were parsed and examined to determine the total volume and type of artifacts retrieved. The data were accessed again using the same forensic tools to inspect their structure and identify relationships among the evidence elements.

5) Analysis: This stage evaluates visual evidence authenticity to identify indicators of fraudulent activity. Four perceptual hashing algorithms aHash, dHash, pHash, and wHash are applied to compressed product images extracted from the Shopee application. Image similarity is measured using normalized Hamming distance (D_h), where lower values indicate stronger visual consistency. Following the validation logic shown in Fig. 2, calculated distances are compared with algorithm specific thresholds ($D_h \leq T_h$). Threshold values of 0.05 (aHash), 0.08 (dHash), 0.04 (pHash), and 0.06 (wHash) are adopted from prior empirical studies and established calibration results in the literature [11,13,14], which demonstrate reliable discrimination under common compression conditions. Distances below these thresholds are classified as forensically valid evidence, while higher values indicate potential alteration or excessive compression. This threshold based evaluation enables objective and reproducible validation of compressed image evidence, transforming the DFRWS analysis phase into a quantitative, content-based forensic validation process consistent with forensic soundness principles.

6) Presentation: In the final stage, a comprehensive forensic report was compiled in accordance with legal standards. This report summarizes the findings and supports the case with validated evidence, making it admissible in court and suitable for litigation processes.

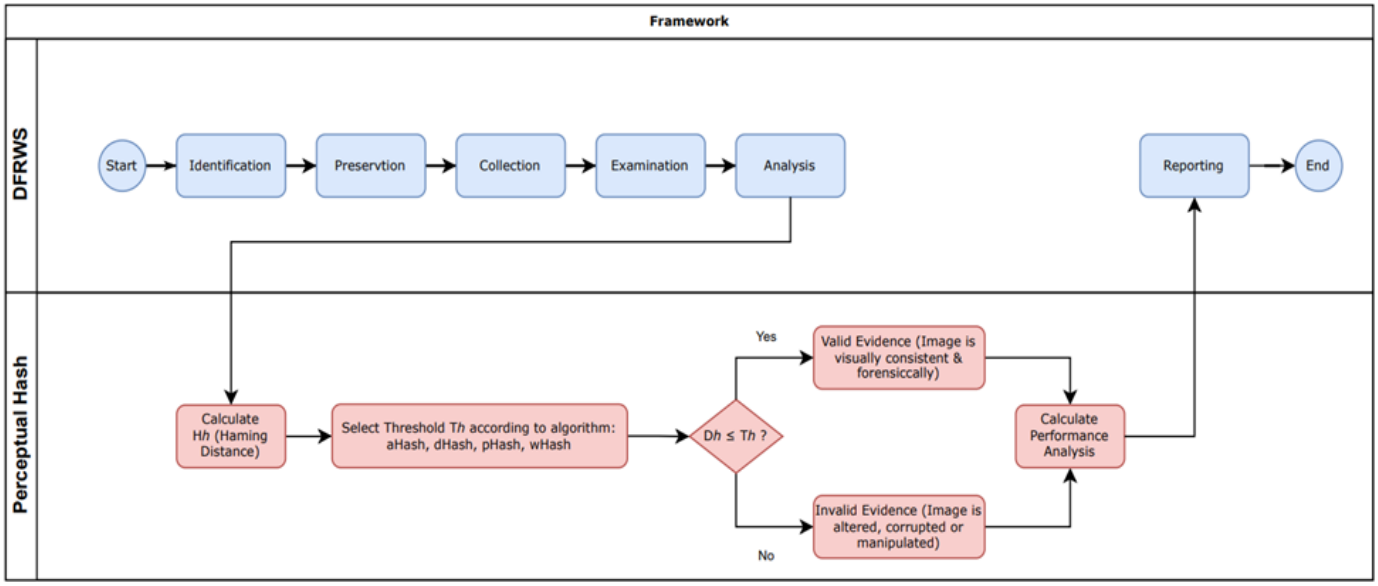

Fig. 2 Perceptual hashing–enhanced DFRWS

C. Performance Analysis

This research adopts a comparative experimental design to evaluate the performance of Oxygen Forensic Detective and MOBILedit Forensic Express, as well as to measure the effectiveness of content based perceptual hashing techniques in validating image evidence extracted from a mobile e-commerce application. The experiment quantitatively assesses accuracy and reliability within the DFRWS based forensic process through four sequential phases: extraction of digital artifacts, image similarity analysis based on normalized Hamming distance, comparative evaluation of recovery and validation rates, and statistical interpretation of forensic tool performance. To maintain analytical objectivity, the study applies standard quantitative metrics commonly used in digital forensic validation, including Accuracy (1), False Positive Rate (2), and False Negative Rate (3), which are mathematically expressed as follows [22].

$$\text{Accuracy} = \frac{\text{TP+TN}}{\text{TP+TN+FP+FN}} \quad (1)$$

$$\text{FPR} = \frac{\text{FP}}{\text{FP+TN}} \quad (2)$$

$$\text{FNR} = \frac{\text{FN}}{\text{FN+TP}} \quad (3)$$

In these equations, TP (True Positive) represents image pairs correctly identified as similar, TN (True Negative) represents image pairs correctly identified as dissimilar, FP (False Positive) denotes dissimilar images mistakenly classified as similar, and FN (False Negative) denotes similar images mistakenly classified as different. These indicators provide an objective foundation for assessing the accuracy, robustness, and reliability of hashing algorithms in validating compressed or transformed images. This research compares four perceptual hashing algorithms aHash, dHash, pHash, and wHash using Accuracy, False Positive Rate (FPR), and False Negative Rate (FNR) as quantitative evaluation metrics to measure performance and resilience against compression. Among these, pHash and wHash demonstrate a higher ability to tolerate compression effects and minor visual transformations [23] ensuring greater consistency of hash values. In contrast, cryptographic algorithms such as MD5, SHA-1, and SHA-256 are excluded, as they operate at the binary level and fail to preserve hash consistency after compression or format conversion. Therefore, this research focuses on content-based digital evidence validation within mobile forensic analysis in accordance with the DFRWS framework, ensuring both technical accuracy and forensic admissibility.

III. RESULT AND DISCUSSION

This research outlines a digital forensic investigation conducted using the complete DFRWS framework, covering all stages from identification to presentation. The approach proves effective in cases where perpetrators alter or delete e-commerce evidence. During the analysis phase, perceptual hashing methods were employed to validate compressed or modified visual artifacts, ensuring that the digital evidence remains authentic, reliable, and legally admissible.

A. Identification

The identification process was conducted under formal legal authorization to ensure evidentiary relevance, with on scene documentation of the smartphone establishing the device's initial condition as a baseline for digital evidence integrity. Within the DFRWS framework, aligned with ISO/IEC 27037 and emphasizing process control and evidential traceability, device isolation, enabling Developer Options, performing a forensic backup, and executing legally authorized rooting were applied as controlled interventions to balance data accessibility and forensic traceability while minimizing alterations to the original source [24,25], as documented in Fig. 3.

B. Preservation

Following the identification stage, the preservation phase represents a critical mechanism to ensure the reliability of digital evidence, particularly for the Samsung SM-G532G device, throughout the investigative process. This approach emphasizes the importance of maintaining the integrity and traceability of evidence, so that each digital artifact from the device can be verified and legally admissible, in accordance with the principles outlined in ISO/IEC 27037 [25]. Within the DFRWS framework, preservation serves as a conceptual control that ensures all subsequent analyses including artifact verification and cryptographic validation are based on evidence that is stable, authentic, and forensically sound.

C. Collection

The acquisition result produced physical forensic imaging that accurately represent the original state of the device data. The imaging generated by Oxygen Forensic Detective and MOBILedit Forensic Express served as the primary data sources for subsequent examination and analytical validation of digital artifacts. A comparative summary of the acquisition results from both forensic tools is presented in Table I, which provides the basis for further analytical evaluation in the following stages.

D. Examination

The examination result assessed the scope and structural characteristics of digital artifacts extracted by each forensic tool. Oxygen Forensic Detective produced a higher volume of system-level artifacts, whereas MOBILedit Forensic Express identified a broader range of artifact categories, including multimedia, location data, and user activity logs, as summarized in Table II. These differences reflect variations in extraction depth and data organization rather than evidentiary inconsistency.

E. Analysis

The analytical results indicate that the extracted communication artifacts are consistent with the simulated fraud scenario and possess strong evidentiary value for legal proceedings. As illustrated in Fig. 4.

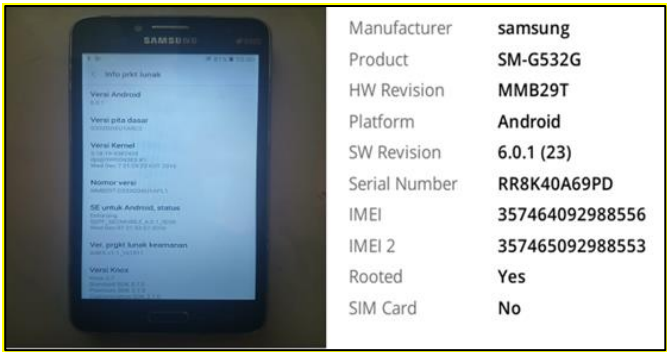

Fig. 3 The perpetrator's device

TABLE I
RESULT OF COLLECTION

Tool	Forensic Image	Size (GB)	Extraction Type
Oxygen Forensic Detective	image_Oxygen Forensic.bin	3.63 GB	Physical extraction
MOBILedit Forensic Express	SM-G532G_MOBILedit Forensic.img	7.28 GB	Physical extraction

TABLE II
RESULT OF EXAMINATION

Tool	Number of Files/Artifacts	Categories
Oxygen Forensic Detective	18.068	11 user accounts, 7 installed applications, 7 user search records, 3,738 OS artifacts
MOBILedit Forensic Express	25.389	Location data, contact lists, multimedia content, user activity logs

Fig. 4 presents a recorded conversation that establishes a clear transactional sequence, demonstrating intent, agreement, and temporal linkage between the parties, which are essential elements for proving fraudulent activity in judicial proceedings. The associated digital artifacts extracted by the forensic tools, as shown in Fig. 5, further support the evidentiary validity of this interaction.

Fig. 5 strengthens the evidentiary context by correlating textual communication with application data and compressed visual artifacts. The extracted images were subject to automatic resizing and compression by the e-commerce platform [5], which altered their cryptographic hash values and reduced the effectiveness of conventional integrity verification [26]. To address this limitation, perceptual hashing was applied using a 32 × 32 representation, enabling content-based validation despite structural modification. The observed cross-artifact consistency supports evidential integrity, reinforces forensic soundness, and satisfies legal admissibility requirements within the DFRWS framework. From a legal perspective, the applied perceptual hashing approach aligns with the Daubert standard [27], as it is testable, reproducible, and supported by measurable error rates derived from accuracy, false positive, and false negative evaluations, thereby strengthening the reliability of digital evidence for judicial proceedings. Complete perceptual hash validation results are presented in Table III.

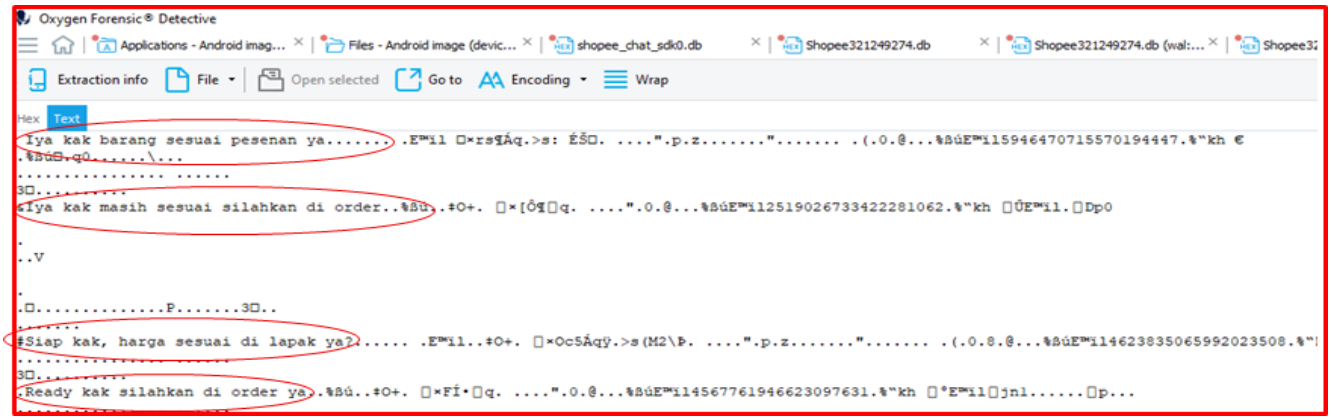

Fig. 4 Result evidence chat

Fig. 5 Result evidence image and video

TABLE III
RESULT OF PERCEPTUAL HASH VALIDATION

Image File	aHash Distance	dHash Distance	pHash Distance	wHash Distance	Conclusion
Image 1	13/0.013	65/0.063	20/0.020	10/0.010	*Similar(a/d/p/w)*
Image 2	6/0.006	29/0.029	14/0.014	108/0.105	*Similar(a/d/p), Different(w)*
Image 3	2/0.002	8/0.008	22/0.021	375/0.366	*Similar(a/d/p), Different(w)*
Image 4	2/0.002	78/0.076	18/0.018	2/0.002	*Similar(a/d/p/w)*
Image 5	4/0.004	81/0.079	16/0.016	2/0.002	*Similar(a/d/p/w)*
Video 1	2/0.002	125/0.122	26/0.025	2/0.002	*Similar(a/p/w), Different(d)*
Video 2	0/0.000	147/0.143	34/0.033	6/0.005	*Similar(a/p/w), Different(d)*

Table III demonstrates that pHash and wHash consistently maintained similarity within threshold limits, confirming resilience to compression. Meanwhile, aHash and dHash showed occasional misclassification particularly on dynamic video frames caused by gradient and luminance variation. These results highlight the superior robustness of perceptual algorithms, especially pHash and wHash, for maintaining evidentiary integrity in mobile forensic analysis.

F. Presentation

At the presentation stage, the researchers outlined the findings, including conversations, user IDs, media files, and group data extracted from the device database. The effectiveness of the forensic tools was evaluated using the index formula (4) to assess their accuracy in retrieving digital evidence [8].

$$\text{Par} = \frac{\sum \text{ar0}}{\sum \text{arT}} \text{ x } 100\% \quad (4)$$

Description:

Par : Accuracy index of the forensic tool used (in percent)

$\sum$ ar$_0$: Number of parameters successfully detected by the tool

$\sum$arT : Total digital evidence parameters used in the analysis process

This research demonstrates that mobile forensics is effective for digital investigations in e-commerce. The performance index results in Table IV reveal differences in effectiveness between Oxygen Forensic Detective and MOBILedit Forensic Express in collecting digital evidence.

Table IV demonstrates a clear performance disparity between Oxygen Forensic Detective and MOBILedit Forensic Express in digital evidence extraction. This research indicates that the observed performance difference is systematic and aligns with theoretical expectations in mobile forensic investigations, rather than being incidental. Oxygen exhibits greater analytical depth by enabling access to encrypted partitions and protected system directories, which allows the recovery of hidden, residual, and partially deleted artifacts. In contrast, MOBILedit shows more limited coverage of system-level data, resulting in a narrower scope of recovered digital artifacts.

This research extends previous work [5] by applying the DFRWS framework, which ensures legally compliant rooting procedures and enables more comprehensive and technically rigorous forensic analysis [24]. Such integration reinforces legal admissibility and methodological credibility, thereby strengthening the precision of forensic interpretation. Nevertheless, existing forensic tools continue to face structural limitations in fully acquiring artifacts from mobile e-commerce platforms due to multi-layered encryption and automated compression mechanisms that may obscure or transform critical digital evidence.

The analytical findings presented in Table V indicate that integrating perceptual hashing algorithms contributes to the development of an adaptive forensic validation model. This model not only quantifies accuracy but also evaluates algorithmic resilience against compression and minor visual transformations. Consequently, perceptual hashing serves as a robust quantitative framework that enhances evidential reliability, analytical transparency, and legal credibility within DFRWS-based mobile forensic investigations.

TABLE IV
COMPARISON OF DIGITAL EVIDENCE ACQUISITION RESULT OXYGEN FORENSIC AND MOBILEDIT FORENSIC

Types of Digital Evidence	Total	Oxygen Forensic	MOBILEdit Forensic
Account	2	2	2
Chat	12	6	3
Image	5	5	5
Video	2	2	2
Total	21	15	12
Result	**100%**	**71.4%**	**57%**

TABLE V
PERFORMANCE METRICS OF HASHING ALGORITHMS

Algorithm	Accuracy	FPR (%)	FNR (%)	Robustness to Compression	Evaluation Result
pHash	100	0	0	High	Reliable for detecting content preserving transformations
wHash	71.4	0	28.6	Moderate	Effective but less stable under high compression
aHash	100	0	0	High	Consistent and stable under compression
dHash	71.4	0	28.6	Moderate	Sensitive to structural and luminance variations

Table V presents the performance metrics of perceptual hashing algorithms applied to validate compressed image evidence. The results demonstrate that pHash and aHash achieve the highest accuracy and robustness, maintaining stable hash similarity under compression, while dHash and wHash exhibit higher false-negative rates (28.6%), indicating greater sensitivity to aggressive visual distortion. The zero false-positive rate (FPR = 0%) across all algorithms confirms that the selected thresholds effectively distinguish authentic images from altered ones, thereby supporting reliable evidentiary discrimination within forensic analysis. Although the evaluation is conducted on a limited dataset consisting of five images and two video samples, this controlled experimental design is intentionally employed to observe hashing behavior under platform-level compression rather than to achieve large-scale statistical generalization. This approach is consistent with prior research**,** which emphasizes the use of controlled datasets to analyze robustness, similarity stability, and error characteristics of perceptual hashing under transformation scenarios [23,28].

The obtained results are consistent with existing research, which reports that perceptual hashing algorithms particularly pHash and aHash emonstrate superior resilience to compression, resizing, and format conversion compared to cryptographic hashing methods that fail under content-preserving transformations [23,28,29]. Large scale evaluation research further confirms that perceptual hashing maintains low Hamming distance variance for visually similar images, even when subjected to lossy compression, supporting its suitability for forensic image validation [23].

False negative occurrences in this study are primarily attributed to extreme compression levels applied by the Shopee application, which eliminate fine-grained visual features and disrupt pixel based similarity detection. Similar limitations have been documented in prior works, which highlight the trade off between compression tolerance and structural detail preservation in perceptual hashing [29]. This finding underscores the necessity for adaptive threshold calibration or hybrid validation strategies to improve robustness under high compression conditions.

Overall, these analytical results support the development of an adaptive forensic validation model that integrates multi algorithm perceptual hashing within the DFRWS framework. Such integration enhances evidential reliability, analytical transparency, and legal defensibility by enabling content-based verification of compressed visual evidence. Future research should expand dataset scale and explore hybrid or machine-learning-assisted perceptual hashing frameworks to further strengthen statistical validity and establish a standardized digital evidence validation approach for mobile forensic investigations.

IV. CONCLUSION

This research, grounded in the Digital Forensic Research Workshop framework, provides analytical insight into mobile digital forensic investigation of e-commerce fraud on the Shopee platform. Two forensic tools, Oxygen Forensic Detective and MOBILedit Forensic Express, were comparatively evaluated to extract and analyze transaction-related artifacts from the suspect's smartphone. The findings demonstrate that Oxygen achieved deeper system-level access through physical extraction, whereas MOBILedit was limited to logical acquisition, resulting in lower recovery performance. To ensure evidential integrity, the study introduced a quantitative validation approach using four perceptual hashing algorithms aHash, dHash, pHash, and wHash to assess the authenticity of compressed visual artifacts. The evaluation results revealed that pHash and aHash maintained consistent accuracy and robustness under compression, while dHash and wHash exhibited higher false-negative rates due to sensitivity to visual distortion. These outcomes confirm that perceptual hashing provides a reliable and forensically defensible mechanism for validating multimedia evidence within the DFRWS based investigation process. Future research should expand dataset scale and explore hybrid or machine-learning-assisted perceptual hashing frameworks integrated within ACPO and DFRWS methodologies to improve statistical validity and establish a standardized digital evidence validation approach for mobile forensic investigations.

REFERENCES

[1] Kementerian Perdagangan Republik Indonesia, "Statistik Perdagangan E-Commerce 2023," 2023. Accessed: Aug. 03, 2025. [Online]. Available: https://www.kemendag.go.id/

[2] DataIndonesia.id, "Jumlah Pengunjung Shopee Indonesia Q2 2022." Accessed: Aug. 03, 2025. [Online]. Available: https://dataindonesia.id

[3] I. Riadi, Herman, and N. H. Siregar, "Mobile Forensic Analysis of Signal Messenger Application on Android using Digital Forensic Research Workshop (DFRWS) Framework," *Ingenierie des Systemes d'Information*, vol. 27, no. 6, pp. 903–913, Dec. 2022, doi: 10.18280/ISI.270606.

[4] I. Riadi, A. Yudhana, and Galih Pramuja Inngam Fanani, "Comparative Analysis of Forensic Software

on Android-based MiChat using ACPO and DFRWS Framework," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 7, no. 2, pp. 286–292, Mar. 2023, doi: 10.29207/resti.v7i2.4547.

[5] R. Prambudi, I. Riadi, and Murinto, "Analisis Forensik Mobile pada Aplikasi E-Commerce Menggunakan Metode Association of Chief Police Officers: Mobile Forensic Analysis Of E-Commerece Applications Using The Association Of Chief Police Officers Method," *Cyber Security dan Forensik Digital*, vol. 8, no. 1, pp. 44–52, Jun. 2025, doi: 10.14421/csecurity.2025.8.1.5234.

[6] K. Lakshmi, P. Honnavalli, and S. Rajashree, "Ensure the Validity of Forensic Evidence by Using a Hash Function," Singapore: Inventive Communication and Computational Technologies, vol 145. Springer, Singapore., Jan. 2021, pp. 341–346. doi: 10.1007/978-981-15-7345-3_28.

[7] M. Hema and S. P. Shyry, "Efficient Compression of Multimedia Data using Lempel–Ziv–Markov Chain Adaptive Block Compressive Sensing (LZMC-ABCS)," *Wirel Pers Commun*, vol. 135, 2024, doi: 10.1007/s11277-024-11187-z.

[8] M. Muammar, I. Riadi, and R. Umar, "Mobile Forensics in Human Trafficking Investigation Services Using Mobile Laboratory," *JUITA: Jurnal Informatika*, vol. 13, no. 1, pp. 1–10, Mar. 2025, doi: 10.30595/juita.v13i1.24060.

[9] D. Setiawan and I. Riadi, "Mobile Forensic WhatsApp Services in Online Fraud Cases using Digital Forensic Research Workshop Methods," *Int J Comput Appl*, vol. 186, no. 34, pp. 49–56, Aug. 2024, doi: 10.5120/ijca2024923908.

[10] M. Moreb, M. Shadeed, S. Younis, and A. Khalil, "Mobile Forensic Investigation for WhatsApp," in *Practical Forensic Analysis of Artifacts on iOS and Android Devices: Investigating Complex Mobile Devices*, Berkeley, CA: Apress, 2022, pp. 281–328. doi: 10.1007/978-1-4842-8026-3_9.

[11] L. Twenning, H. Baier, and T. Göbel, "Using Perceptual Hashing for Targeted Content Scanning," *IFIP Adv Inf Commun Technol*, vol. 687 AICT, pp. 125–142, 2023, doi: https://doi.org/10.1007/978-3-031-42991-0_7.

[12] M. Offtermatt, M. R. Kilidjian, and L. McGuiness, "Future-proofing Metadata at Los Alamos National Laboratory," in *Proceedings of the International Conference on Dublin Core and Metadata Applications*, Dublin Core metadata initiative, 2024. doi: 10.23106/dcmi.952460454.

[13] S. Sharma, "Analysis of Perceptual Hashing for Threshold Values," *Procedia Comput Sci*, vol. 260, pp. 1107–1112, Jan. 2025, doi: 10.1016/J.PROCS.2025.03.295.

[14] M. Alkhowaiter, K. Almubarak, and C. Zou, "Evaluating Perceptual Hashing Algorithms in Detecting Image Manipulation Over Social Media Platforms," in *2022 IEEE International Conference on Cyber Security and Resilience (CSR)*, 2022, pp. 149–156. doi: 10.1109/CSR54599.2022.9850288.

[15] U. S. D. of H. Security, "Test Results for Mobile Device Acquisition Tool: Oxygen Forensic Detective v17.1.0.131," NIST Computer Forensics Tool Testing (CFTT) Program, United States, May 2025. Accessed: Aug. 03, 2025. [Online]. Available:https://www.dhs.gov/sites/default/files/2025 05/25_0501_st_test_results_for_mobile_device_acqui sition_tool_oxygen_forensic_detective_v17.1.0.131.p df

[16] R. M. Abou-Elzahab, M. F. Al Rahmawy, and T. T. Hamza, "Comparative Study of Different Mobile Forensic Tools for Extracting Evidence from Android Devices," *Mansoura Journal for Computer and Information Sciences*, vol. 16, no. 1, pp. 1–12, 2020, doi: 10.21608/mjcis.2020.321070.

[17] T. Sutikno and I. Busthomi, "Power of analytic tools in Oxygen Forensic ® Detective based on NIST cybersecurity framework," *Computer Science and Information Technologies*, vol. 6, no. 1, pp. 8–19, 2025, doi: 10.11591/csit.v6i1.pp8-19.

[18] F. Breitinger, J.-N. Hilgert, C. Hargreaves, J. Sheppard, R. Overdorf, and M. Scanlon, "DFRWS EU 10-Year Review and Future Directions in Digital Forensic Research," *Forensic Science International: Digital Investigation*, vol. 48, p. 301685, 2024, doi: https://doi.org/10.48550/arXiv.2312.11292.

[19] Y. Jia, C. Cui, and A. A. A. El-Latif, "Robust Image Hashing Using Histogram Reconstruction for Improving Content Preservation Resistance and Discrimination," *Symmetry (Basel)*, vol. 15, no. 5, May 2023, doi: 10.3390/sym15051088.

[20] S. McKeown, P. Aaby, and A. Steyven, "PHASER: Perceptual hashing algorithms evaluation and results - An open source forensic framework," *Forensic Science International: Digital Investigation*, vol. 48, p. 301680, Mar. 2024, doi: 10.1016/J.FSIDI.2023.301680.

[21] H. Mareen, N. Van Kets, P. Lambert, and G. Van Wallendael, "Fast fallback watermark detection using perceptual hashes," *Electronics (Switzerland)*, vol. 10, no. 10, May 2021, doi: 10.3390/electronics10101155.

[22] A. F. Akbar, P. D. W. Ayu, and D. P. Hostiadi, "Performance Analysis of Deep Learning Architectures in Classifying Fake and Real Images," *JUITA: Jurnal Informatika*, vol. 13, no. 2, pp. 167–176, Aug. 2025, doi: 10.30595/juita.v13i2.25790.

[23] S. McKeown and W. J. Buchanan, "Hamming distributions of popular perceptual hashing techniques," *Forensic Science International: Digital Investigation*, vol. 44, Mar. 2023, doi: 10.1016/j.fsidi.2023.301509.

[24] A. Alyas, A. Ahmed, and V. Kumar, "Lawfully Data Collection Techniques in Mobile Forensic & Analysis Using Cellebrite Physical Analyzer," in *Proceedings of the KILBY 100 7th International Conference on Computing Sciences 2023 (ICCS 2023)*, May 2023. doi: 10.2139/ssrn.4483864.

[25] H. Syahida Alawi, I. Riadi, and S. Sunardi, "Improving Credibility of Digital Evidence Investigation in E-Commerce Fraud Cases using ISO/IEC 27037," *International Journal of Advances in Data and Information Systems*, vol. 6, no. 2, pp. 479–495, doi: 10.59395/ijadis.v6i2.1408.

[26] S. Almotiri, *Forensic Hash Value Guidelines: Why Md5 and SHA1 should no longer be used and a recommendation for their replacement*. Auckland University of Technology, 2022.

[27] M. D. Cicchini, "The Daubert Double Standard," Feb. 2021, *Social Science Research Network*. Accessed: Dec. 15, 2025. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3787772

[28] P. Samanta and S. Jain, "Analysis of Perceptual Hashing Algorithms in Image Manipulation Detection," *Procedia Comput Sci*, vol. 185, pp. 203–212, 2021, doi: https://doi.org/10.1016/j.procs.2021.05.021.

[29] Y. Jakhar and M. D. Borah, "Effective near-duplicate image detection using perceptual hashing and deep learning," *Inf Process Manag*, vol. 62, no. 4, p. 104086, 2025, doi: https://doi.org/10.1016/j.ipm.2025.104086.