Journal of Information Systems and Informatics
Vol. 7, No. 1, March 2025 e-ISSN: 2656-4882 p-ISSN: 2656-5935
DOI: 10.51519/journalisi.v7i1.882 Published By DRPM-UBD

Forensic Investigation of Drug and Food Crimes in Digital Marketplace

Adinda Meutia[1], Ahmad Luthfi[2,*]

[1,2]Master Program of Informatics, Faculty of Industrial Technology, Universitas Islam Indonesia, Indonesia
Email: [1]21917001@students.uii.ac.id, [2]ahmad.luthfi@uii.ac.id*

Abstract

This research holds great significance as it is anticipated to safeguard customers from harmful frug and food products in cyberspace and to enforce the law by offering solid evidence to bring criminals to justice. Furthermore, this research helps to better understand how crimes that take place in the marketplace are committed, which enables the implementation of more effective preventive measures. Besides, in order to combat cybercrime, the findings of this study may serve as the foundation for the creation of more effective digital forensic investigation techniques. In order to perform digital forensic investigations of drug and food offenses using the marketplace, this study aims to develop an efficient and successful model or implementation guideline. This seeks to methodically direct the inquiry process while adhering to relevant norms. The objective of this research endeavor is to provide a model or practical guideline that is both effective and efficient for using the marketplace to undertake digital forensic investigations of drug and food crimes. This seeks to methodically direct the research process while adhering to relevant criteria. The following stages make up the Design Science Research (DSR) method of research: The issue in this project is "How to conduct a digital forensic investigation for Drug and Food crimes using the marketplace so that it can be used as evidence in court?" Then, in order to adopt answers from related research and make adjustments linked to research difficulties, a literature review is conducted to locate prior research. A model or implementation guideline for performing digital forensic investigations of the marketplace is the type of solution or artifact anticipated in this project. The next phase is solution design, which involves using an existing forensic investigation framework to create an artifact design. Following every step of the framework, case study experiments are then conducted to test the artifact design. The examination of the artifact design by both experts and consumers is the last phase.

Keywords: Digital Forensics, Marketplace, Drug and Food, Crime, Cyberspace

1. INTRODUCTION

Businesses use marketplace because they are convenient, require little capital, and have a large buyer base. Furthermore, because a third party handles the payment mechanism, purchasers feel safer when making purchases [1]. In order to win over

customers, dealers of illicit goods also make use of the characteristics offered by this marketplace. Additionally, the marketplace just shows the store name and the sales location area, with no open disclosure of the seller's identity [1]. To evade law enforcement oversight, the sale of prohibited goods is typically not conducted publicly or transparently to all customers. Because of this, the market for illegal goods is constrained, and in an effort to grow, transactions are conducted through e-commerce platforms, particularly marketplace, which create challenges for law enforcement officers [2].

Currently, the Food and Drug Monitoring Agency (BPOM) with its cyber patrol unit is responsible for monitoring the online circulation of illegal drugs and food due to the very rapid growth of e-commerce in Indonesia in 2018 [3]. According to the cyber patrol's findings, drug and food crimes are committed through the marketplace platform. Crimes involving the production and/or distribution of drugs and food that do not possess a BPOM distribution permission, include hazardous chemicals, or fail to meet safety, quality, and efficacy standards are known as drug and food crimes.

The terms "drugs and food" in this context refer to pharmaceuticals, narcotics, psychotropics, precursors, addictive substances, conventional medications, health supplements, cosmetics, and processed foods. During 2021, the Drug and Food Supervisory Agency's Deputy for Enforcement said that they had discovered 286,844 e-commerce links that violated the laws pertaining to food and drugs, which were then reported to the appropriate authorities for removal [4]. As the organization in charge of overseeing food and drug distribution in Indonesia, BPOM faces more difficult problems in combating the crime of illegal food and drug distribution through the marketplace. Law enforcement needs solid and reliable evidence to use in the trial process against those who commit this crime. Digital forensic investigations are therefore crucial for gathering electronic evidence that can be presented in court.

This study combines digital forensic investigation standards, namely ISO/IEC 27042:2015, ISO/IEC 27037:2012, and ISO/IEC 27043:2016. The integration of these standards aims to propose a framework for investigating illicit drugs in marketplace. The guidelines in ISO/IEC 27042:2015 cover continuity, validity, reproducibility, and repeatability in the analysis and interpretation of digital evidence [5]. Identification, collection, acquisition, and preservation of potentially useful digital evidence are among the specific tasks in the management of digital evidence that are outlined in ISO/IEC 27037:2012 [5]. The instructions in ISO/IEC 27043:2015 are based on idealized models for standard incident investigation procedures in a variety of digital evidence incident investigation scenarios.

Therefore, the suggested investigation model in this study helps to guide the investigation process in a methodical manner while adhering to pertinent standards. Furthermore, the established framework can serve as a practical and efficient guideline for performing digital forensic investigations for possible food and drug crimes in marketplace. Therefore, in order to guarantee a robust framework, this study employs the Design Science Research (DSR) research method, which is full of useful aspects and can adapt the interactive digital forensic investigation process.

2. RELATED WORKS

To begin looking for a solution, researchers reviewed a number of relevant empirical studies in the literature. The field of marketplace forensic analysis is currently the subject of many investigations. Dorai et al.'s study discusses forensic analysis for applications used in marketplace around the world. They found that digital artifacts of user data and transaction activity on Amazon and Etsy applications on jailbroken iOS X and rooted Android 9 smartphones [6]. On a rooted Android 8 smartphone, forensic analysis was used in another study to extract personally identifiable information from eight popular marketplace applications in Pakistan related to delivery, transportation, and product purchasing: Daraz.pk, Airlift Express, GrocerApp, Clicky Online Shopping, Bykea, Uber, Indriver, and Foodpanda. These devices were chosen because, in the Android 10 experiment, no newly installed application data was found, and on Android 8 with a different type of smartphone, the data obtained could not be opened due to encryption [7]. The purpose of Kiptoo's study is to provide a framework for forensic analysis of Android smartphones used by marketplace applications related to transportation, specifically Uber, Little, and Bolt. The universality, validity, and efficacy of the research framework were then evaluated [8]. A forensic investigation of the Wish Android Marketplace app was the subject of another study in 2019 that uncovered digital locations and artifacts as well as user, transaction, and credit or debit card data [9].

In a study by Hayes et al., the security of the Uber app for users was examined. Static and dynamic forensic analysis techniques were applied to the app on iOS and Android devices, and the items that were sought were contacts, locations, and permissions that the app requested to access device hardware, including cameras and microphones, as well as user personal information [10]. The study conducted by Nasution et al. focused on social media, but it also looked into Android users [11]. Anwar et al.'s research used the same research object as this plan, which is the Indonesian marketplace application on Android devices. Anwar's research examined the security system and found access permissions to assess each application's risk level [12]. The ADAM technique was used by Wibowo et al. to investigate non-public cloud computing, and Luthfi & Prayudi conducted a

number of pertinent research pertaining to the forensic investigation readiness process model for the preservation of digital evidence [13]. A conceptual model component of internet forensic investigations is enhanced by the findings of these two research. Nevertheless, they haven't yet addressed the e-Commerce case in detail [14].

In order to offer a more thorough understanding of forensic investigation of marketplace apps, these empirical research studies enhance one another. By linking the results of many investigations, we may comprehend the various situations in which forensic investigation techniques are used as well as how the advancement of security regulations and technology affects the efficacy of forensic analysis methods.

In their study, Dorai et al. demonstrated how forensic analysis might reveal digital artifacts from user transactions on popular marketplace apps like Amazon and Etsy, suggesting that rooted or jailbroken smartphones can provide access to transaction data and personal information. These results are in line with those of another study that looked into Pakistani marketplace apps, where rooted Android eight smartphones could potentially retrieve sensitive data like transaction history and personal identities. Both investigations verify that weaknesses in the data management of marketplace apps give forensic analysts access to vital data, offering important information about initiatives to strengthen user data security. A crucial component of creating future forensic investigation techniques is recognizing how operating system evolution contributes to security risk mitigation, as evidenced by the variations in results across more recent Android versions.

Kiptoo's research adds credence to earlier findings by putting out a forensic methodology for examining transportation apps that function within an ecosystem of service-based marketplace, like Uber, Little, and Bolt. In addition to the empirical approach used in earlier research, this study offers a more systematic view on forensic investigative techniques by assessing the framework's universality, validity, and effectiveness. The study by Hayes et al., on the other hand, combines both static and dynamic forensic analysis approaches to find possible exploitation of location data and hardware access rights, with an emphasis on the Uber application's security and its effect on user privacy. In relation to Kiptoo's research, these findings show that applications for transportation-based marketplace not only save transaction data but also run the risk of disclosing private information that users have authorized access to.

Additionally, Anwar et al.'s study particularly looked at Android applications from the Indonesian marketplace and discovered variations in risk levels depending on the access rights that the program asked for. Similar to this, Nasution et al.'s study examined the security trends of Android apps generally, despite having a greater

emphasis on social media. Moreover, the ADAM technique, which Wibowo et al. employed to study non-public cloud computing, can serve as a guide for comprehending the processing and security of user data kept in cloud infrastructure. Likewise, Luthfi and Prayudi's forensic investigative preparedness process model emphasizes the significance of digital evidence preservation in a wider context. As a result, including these data offers a solid basis for the future development of more efficient inquiry techniques while also enhancing knowledge of the prospects and difficulties in marketplace forensic analysis.

3. METHOD

The problem-solving approach and strategy in this study is to develop a model/implementation guideline in conducting digital marketplace forensic investigations for drug and food crimes that are effective, efficient, and in accordance with applicable rules. With clear and structured guidelines, it is hoped that the digital forensic investigation process can be carried out more systematically and accurately, so that the electronic evidence found can be a strong basis in the law enforcement process. Active participation from stakeholders will be key in developing this implementation guideline.

This study will explore feedback from various parties, including digital forensic experts, law enforcement, and representatives from the online marketplace platform itself. By receiving input from various perspectives, we can ensure that the resulting implementation model/guideline is not only theoretical, but also practical in the context of routine investigations. In this case, researchers must be able to identify specific research problems and provide strong arguments regarding the relevance of the background of the problem and the importance of exploration and efforts to solve it. In the context of this study, the problem identified is how to conduct a digital forensic investigation for drug and food crimes using the marketplace so that it can be used as evidence in court. The DSR approach used in this study assists in the development and performance of artifacts with a more explicit goal of improving the functional performance of artifacts [15]. This research is a cross-disciplinary study, including cybersecurity, data science, and digital forensics. Therefore, DSR has an important role in understanding stakeholder needs, user behavior and experience, especially through a qualitative approach.

After identifying the problem, the next step is to find a solution. Researchers must conclude the purpose of the solution by analyzing the problem description and understanding its feasibility. In this study, although no pre-existing solutions were found that were specific to the research problem, researchers can adopt solutions from similar studies and adjust related to the research problem. The form of solution or artifact produced from this study is expected to provide a significant

contribution in the field of digital forensic investigations related to drug and food crimes using the marketplace. The output is in the form of determining the type of artifact and components as a solution to the problem, at this stage a survey was conducted with stakeholders.

4. RESULTS AND DISCUSSION

4.1. Conceptual Model

In this study, we developed a conceptual model and implementation training to conduct digital forensic market research. The conceptual model and implementation guidelines are based on the standards for initial evidence handling, digital evidence analysis and interpretation, and laboratory digital forensic procedures that comply with relevant standards. Digital forensics implementation usually consists of three stages: initial evidence processing, digital evidence analysis and interpretation, and reporting that complies with relevant standards. In this case, when creating the implementation guidelines, the researcher referred to three standards, namely ISO/IEC 27032, 27042, and 27043, which are related to cybersecurity and digital forensic investigations. As depicted in Figure 1, the following is the actual market situation as viewed through the perspective of food and drug cybercrime.

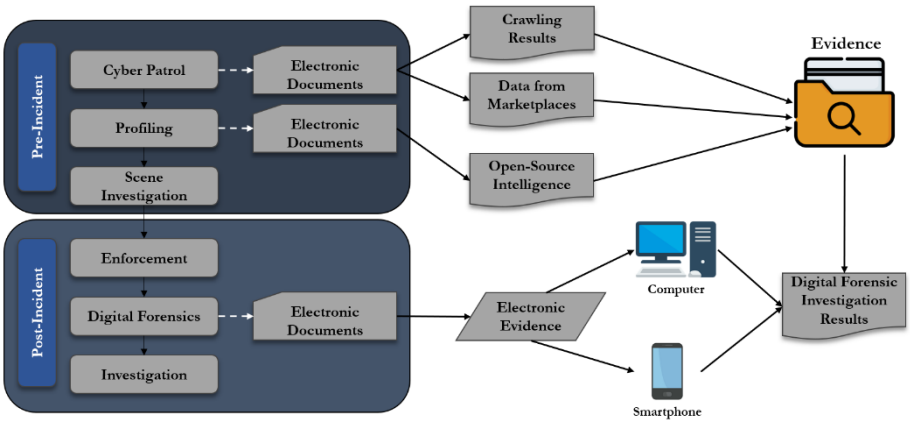

Figure 1. Real Case Situation of Drug and Food Cybercrime in the Marketplace

Several factors can be explained by looking at the field circumstances shown in Figure 1. First, the pre-incident phase consists of three activities: (1) cyber patrol, which is an attempt to gather information or electronic documents in the marketplace about drug violations or counterfeiting without a distribution permit; (2) profiling of multiple marketplace accounts that may be targets due to suspicions of violation character; and (3) field investigations, where the cyber patrol team

carries out technical in-depth investigations. There are a number of ways to track down this evidence, including (a) crawling, which is how a search engine locates information that has been updated on a marketplace website; and (b) gathering information from the marketplace utilizing open-source intelligence to uncover evidence sources from the target marketplace account. This stage involves the acquisition of several artifacts, such as transaction history, account owner profile information, and a number of advertising showcases accused of violating drug laws without a distribution permission.

Second, there are three stages in the post-incident phase: (1) action, which is an activity in which law enforcement officers and field investigators collaborate to take direct action in the field following information about suspected drug-related evidence at locations without a distribution permit. The investigation team conducts crime scene processing activities (TKP) at this point in order to gather any possible electronic devices that were present at the scene at that moment; (2) following this, the team transports the confiscated electronic devices to the Digital Forensic Laboratory, Directorate of Cyber Drugs and Food, BPOM RI. At this point, the confiscated devices—such as computers or smartphones—then conduct additional business process investigation in the laboratory, and (3) the final activity was an investigation that involved a number of activities, such as (a) acquiring electronic devices to obtain imaging files, which are files that were obtained by scanning or copying the electronic device from its original source, and (b) extracting and analyzing potential evidence in line with the case being prosecuted. In order to gather crucial information, investigators at this stage perform analysis based on their knowledge and experience. They then offer evidence notes on possible digital evidence, and they interpret the findings of the analysis of digital evidence using their knowledge and experience. Whether or not the analysis's findings are shown to be identical to the owner of the electronic device's evidence, for instance, and (d) documenting or creating an investigation report, this is the most important stage where investigators are asked to offer their opinions and knowledge objectively. As the last phase, this stage is also crucial because it is when investigators produce at least three reports: a technical report, an analysis and interpretation report, and an investigative report. The upcoming legal procedure is predicated on this report. Furthermore, this study develops a framework that the investigation team can utilize to conduct digital forensic investigations. The international standards ISO/IEC 27037 and ISO/IEC 27042, which outline the process from preparedness, initiation, acquisition, inquiry, identification, retrieval, analysis, and interpretation, were modified to create this framework.

This stage highlights the importance of careful documentation and chain of custody management in addition to the reports and framework. From the gathering of evidence to the final analysis, thorough documentation guarantees that every step of the investigation is documented. This openness is essential for preserving

the investigation's integrity as well as making sure the evidence is strong enough to stand up in court. Any improper handling or missing documentation could possibly damage the evidence's credibility in court, which could result in objections to the conclusions or even their rejection.

Additionally, the framework encourages uniformity and reproducibility in digital forensic investigations by conforming to ISO/IEC 27037, ISO/IEC 27042 and ISO/IEC 27043. This implies that other teams or investigators can provide results that are comparable in the future by using the same structured technique. Because it creates a common ground for cooperative efforts, this degree of consistency is especially crucial in situations involving numerous jurisdictions or cross-border inquiries. In the end, this method improves the general effectiveness and dependability of digital forensic investigations while also fortifying the judicial system. An example of the framework developed in this study is shown in Figure 2.

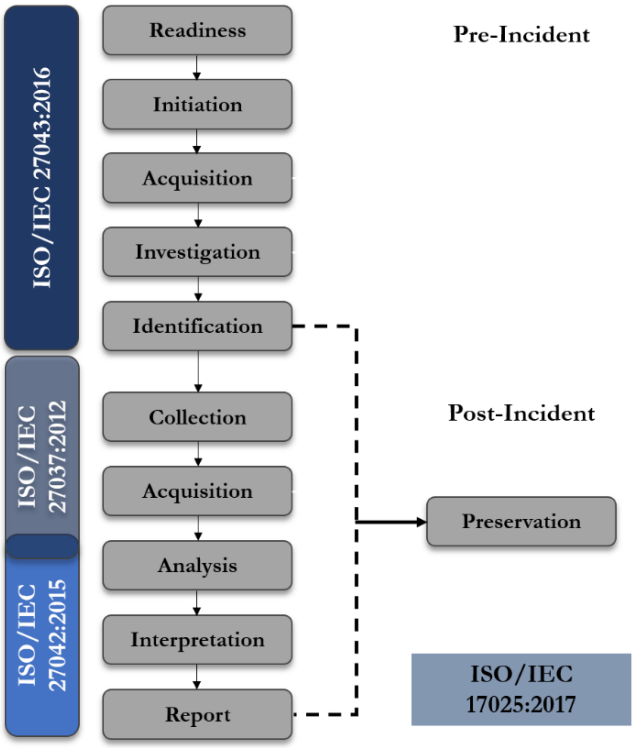

Figure 2. Proposed Framework for Investigation of Unlicensed Drugs in the Marketplace

4.2. Discussion

The conceptual model and implementation guidelines proposed in this study serve as a critical milestone in enhancing digital forensic procedures specific to

cybercrime in food and drug marketplaces. The integration of international standards such as ISO/IEC 27032, 27042, and 27043 has provided a structured and reliable foundation for handling digital evidence, particularly within the unique context of online drug violations. This discussion elaborates on the significance, implications, and real-world relevance of the findings by dissecting the framework into actionable and strategic layers.

First and foremost, the dual-phase structure—pre-incident and post-incident—emphasizes a proactive and reactive synergy, which is crucial in today's digital crime landscape. The pre-incident phase, involving cyber patrol, account profiling, and field investigations, highlights the necessity of anticipating and identifying threats before they manifest into severe legal or public health risks. The practical application of web crawling and open-source intelligence reflects a modernized approach to surveillance, capable of navigating the rapid, decentralized nature of online marketplaces. Notably, the ability to extract transaction histories, advertising showcases, and user profile information supports a more evidence-backed, data-driven methodology that strengthens pre-raid investigations.

Moving into the post-incident phase, the implementation of swift, tactical field actions, followed by the secure transportation and forensic examination of electronic devices, marks a significant improvement in preserving digital evidence integrity. The study reinforces the importance of a structured workflow—from acquisition and imaging to analysis and reporting—mirroring a well-orchestrated chain of custody. Each sub-phase contributes to a seamless transition between field action and laboratory investigation, where even the minutest details can critically affect case outcomes.

What stands out most prominently in this framework is its capacity to maintain evidence reliability through standardization. Adhering to ISO/IEC 27037 and 27042 in the analysis and interpretation phase ensures that evidence remains consistent, traceable, and legally defensible. This is particularly vital when handling sensitive cases that may involve multiple jurisdictions or international actors. The uniform procedures not only enhance reproducibility across investigation teams but also mitigate risks of procedural discrepancies that might weaken legal claims.

Moreover, the emphasis on meticulous documentation and chain of custody management throughout the digital forensic process cannot be overstated. The value of transparent, step-by-step logging ensures that every action taken on digital evidence can be accounted for, audited, and defended in court if necessary. From an evidentiary standpoint, this level of transparency safeguards investigators against potential legal challenges, bolstering the judicial weight of their findings. Missing or incomplete records, by contrast, can severely compromise the

admissibility of evidence, potentially derailing entire investigations and court proceedings.

Another significant strength of the developed framework is its scalability and adaptability. The methodology allows for consistent application across various platforms and investigation teams, enabling coordination in broader cybercrime operations. As digital crime evolves, this flexibility is essential for staying ahead of criminal tactics. More importantly, having a structured, repeatable framework empowers forensic investigators to operate confidently, knowing their methods meet international scrutiny.

The study also underlines the necessity of human expertise in interpreting digital evidence. Despite technological advancements in forensic tools, the nuanced interpretation of data—determining its context, relevance, and authenticity—still relies heavily on the knowledge and experience of investigators. This hybrid approach, combining human judgment with standardized digital processes, reflects a balanced methodology that maximizes reliability and accuracy.

In practical application, the proposed framework for investigating unlicensed drug transactions in online marketplaces, as illustrated in Figure 2, serves not only as a procedural guide but also as a policy blueprint. Law enforcement agencies and regulatory bodies like BPOM RI can utilize this framework to optimize their investigative workflows and enhance collaboration across departments. Furthermore, by aligning forensic procedures with international standards, the framework increases the potential for successful legal prosecution, ultimately safeguarding public health from the threats of counterfeit or unauthorized pharmaceuticals.

Finally, the conceptual model and guidelines presented in this study represent a well-rounded, standards-compliant, and contextually relevant approach to digital forensic investigation in food and drug cybercrime. By leveraging a combination of proactive cyber intelligence, structured forensic processing, and internationally recognized best practices, the framework strengthens both investigative integrity and legal enforceability. This approach not only contributes to the broader fight against cybercrime but also sets a benchmark for future digital forensic implementations across related sectors.

5. CONCLUSION

The final section of this paper outlines the essential steps for pre- and post-event digital forensic investigations, particularly in drug cases involving the unlawful distribution of narcotics through online marketplace. The pre-incident phase focuses on cyber patrol, profiling, and field investigations using advanced methods

like data crawling and open-source intelligence to get crucial evidence. Digital evidence is collected, extracted, examined, processed, and recorded during the post-event stage. Additionally covered are thorough digital forensic analysis and crime scene processing in specialized labs.

The study also offers a framework based on ISO/IEC 27037 and 27042 standards that enhances the uniformity, reproducibility, and integrity of digital forensic investigations. Investigators can maintain a strong chain of custody and the admissibility of the evidence in court by adhering to these standards, which ensure that every step of the process is well documented. This meticulous approach is required to prevent any gaps in the research process that can jeopardize the reliability of the findings presented in court.

Moreover, the framework enables collaboration across multiple countries, which makes it very useful for cross-border investigations. By promoting uniformity in the investigative techniques, the framework improves the overall reliability of digital forensic efforts and ensures that the legal process is not only thorough but also effective and efficient. Regardless of the teams or the complexity of the case, this systematic approach can expedite follow-up investigations and yield reliable results.

REFERENCES

[1] E. A. Wibowo, "Pemanfaatan Teknologi e-Commerce Dalam Proses Bisnis," *Equilibria*, vol. 1, no. 1, pp. 95–108, 2014.

[2] M. I. Alghamdi, "Digital Forensics in Cyber Security—Recent Trends, Threats, and Opportunities," in *Cybersecurity Threats with New Perspectives (CSTNP)*, 2021.

[3] William and H. W. Aripradono, "Faktor Keputusan Pembelian Konsumen Online Marketplace Indonesia," *Teknika*, vol. 9, no. 1, pp. 48–57, Jul. 2020, doi: 10.34148/teknika.v9i1.269.

[4] BPOM RI, "Laporan Kinerja 2021 Deputi Bidang Penindakan," Badan Pengawas Obat dan Makanan Republik Indonesia (*BPOM*), Jakarta, 2021.

[5] N. Yalçın and B. Kılıç, "ISO/IEC 27037, ISO/IEC 27041, ISO/IEC 27042 ve ISO/IEC 27043 Standartlarına Göre Sayısal Kanıtlar," in *Proc. 4th Int. Symp. Innovative Approaches Eng. Natural Sci.*, Jul. 2019, pp. 444–449, doi: 10.36287/setsci.4.6.118.

[6] G. Dorai, S. Hutchinson, B. Rodriguez, and U. Karabiyik, "Mobile Commerce - Analysis and Investigation of the Online Safety, Privacy, and Data Forensics of Amazon and Etsy Apps," in *Proc. Hawaii Int. Conf. Syst. Sci.*, 2023, doi: 10.24251/HICSS.2023.533.

[7] S. S. Zehra and S. Qadir, "Forensic Data Analysis of Delivery and Transport Applications," in *Proc. Int. Conf. Cyber Warfare Secur.*, IEEE, Dec. 2022, pp. 62–68, doi: 10.1109/ICCWS56285.2022.9998473.

[8] K. K. Kiptoo, "A Forensic Investigation Framework For Android On-Demand Ride Applications," M.S. thesis, Strathmore Univ., Nairobi, Kenya, 2020.

[9] S. Pasha and S. Saleem, "Forensics Analysis of Wish-Shopping Made Fun Application on Android," in *Proc. Int. Conf. Frontiers Inf. Technol.*, IEEE, Dec. 2019, pp. 144–1445, doi: 10.1109/FIT47737.2019.00036.

[10] D. Hayes, C. Snow, and S. Altuwayjiri, "A Dynamic and Static Analysis of the Uber Mobile Application from a Privacy Perspective," *J. Inf. Syst. Appl. Res.*, vol. 11, no. 1, pp. 11–22, 2018.

[11] M. R. Nasution, Y. Prayudi, and A. Luthfi, "Investigating Social Media User Activity on Android Smartphone," *Int. J. Comput. Appl.*, vol. 183, no. 48, pp. 46–52, Jan. 2022, doi: 10.5120/ijca2022921890.

[12] N. Anwar, S. A. Akbar, A. Azhari, and I. Suryanto, "Ekstraksi Logis Forensik Mobile pada Aplikasi E-Commerce Android," *Mobile Forensics*, vol. 2, no. 1, pp. 1–10, Mar. 2020, doi: 10.12928/mf.v2i1.1791.

[13] A. Luthfi and Y. Prayudi, "Process Model of Digital Forensics Readiness Scheme (DFRS) as a Recommendation of Digital Evidence Preservation," in *Proc. Int. Conf. Cyber Secur., Cyber Warfare Digit. Forensic*, IEEE, Oct. 2015, pp. 117–122, doi: 10.1109/CyberSec.2015.31.

[14] D. K. Wibowo, A. Luthfi, Y. Prayudi, E. Ramadhani, and M. Maulana, "Faux Insider Hazard Investigation on Non-Public Cloud Computing by Using ADAM's Technique," *J. RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 6, no. 6, pp. 1028–1036, Dec. 2022, doi: 10.29207/resti.v6i6.4714.

[15] A. Hevner, S. March, J. Park, and S. Ram, "Design Science in Information Systems Research," *MIS Q.*, vol. 28, no. 1, p. 75, 2004, doi: 10.2307/25148625.