OPEN ACCESS
ISSN 2356-5462
https://journals.telkomuniversity.ac.id/ijoict/

Intl. Journal on ICT
Vol. 11, No. 1, Jun 2025. pp. 79-89
doi.org/10.21108/ijoict.v11i1. 8966

Enhancing Digital Forensics with Cyber Kill Chain and 5W1H: A Case Study on Phishing Attacks

Erika Ramadhani [1*], Toto Raharjo [2]

[1]*Department of Informatics,* [2]*Magister of Informatics-Universitas Islam Indonesia*
Jalan Kaliurang Km.14,5 Yogyakarta, Indonesia

[*] erika@uii.ac.id

Abstract

This research has combined the Cyber Kill Chain (CKC) model and the 5W1 H for detection and control of cybercrime such as phishing for the automation of digital forensic investigation. The most vital challenge in digital forensics is its evidence handling complexity, the lack of a standard because of diversified kinds of tools, and the non-availability of automated tools that systematically present information. Therefore, it provides a web-based framework to automate the investigation by referring to the attack stages of the CKC and identifies the contextual allegories of the incident like who, what, when, where, why, and how through the rule of 5W1H. It includes the problem identification method, collecting and classifying the digital artifacts according to CKC stages, in-depth analysis with the 5W1H framework, and visualization of investigation results for further understanding. A case study of a phishing attack on the Kredivo application was used to evaluate the effectiveness of this approach, where the CKC stages from reconnaissance to actions on objectives were implemented to analyze artifacts such as activity logs and phishing data. The results show that the integration of CKC and 5W1H improves analysis accuracy, generates comprehensive visualizations of artifacts, and strengthens response to attacks. It is expected that this finding would mean a highly significant change in the productivity of forensic investigations by making it easier for analysts and preparing proper documentation education for the court.

Keywords: Digital Forensics, Cyber Kill Chain, 5W1H, Information Extraction, Phishing Investigation

I. INTRODUCTION

DIGITAL forensics is concerned with investigating digital devices and data for legal purposes, and is an important discipline in the digital era, serving the needs of cybersecurity and legal enforcement [1]. Unfortunately, such forensic evidence remains inadmissible in court due to standards and regulations being absent and therefore require the cooperation of the legal and technological domains [2]. The increasing penetration of technology into everyday life means that the stage has now been set for cybercrimes. Such increased activity calls for an investigation [3]. For cyberspace security, digital forensics involves identifying, collecting, analyzing, and reporting digital information associated with computing crimes [4].

Received on 3 Mar 2025. Revised on 15 Apr 2025. Accepted and Published on 11 Jul 2025.

Automation plays a crucial role in improving the efficiency and accuracy of forensic investigations, particularly in cyber and digital forensics. [5] and [6] both emphasize the need for automation in managing the increasing volume of digital evidence, with Hayes specifically highlighting its potential to simplify tasks and solve existing challenges. Paper [7] and [8] further delve into the technical and legal aspects of automation, with Gostojić et al proposing a formal knowledge model for online social network forensics and Bokolo presenting a framework for evaluating automated systems in forensic analysis. These studies collectively underscore the importance of automation in enhancing the effectiveness of forensic investigations.

The limitations of existing forensic tools, such as their focus on technical outputs, lack of standardization, and difficulties in integrating comprehensive reporting elements like the 5W1H, have been widely discussed in the literature [9]–[11]. Recent literature identifies critical limitations in current forensic tools and practices. These include an overreliance on technical outputs, inadequate standardization, and challenges in producing comprehensive investigative reports [9]. Despite the implementation of ISO17025 accreditation, quality management in forensic science remains insufficient in addressing procedural complexities [10]. Specific forensic methods, such as toolmark comparison, have come under scrutiny regarding their scientific reliability and evidentiary validity [11]. While Large Language Models (LLMs) show potential in supporting digital forensic workflows, especially in data processing and classification, they are not substitutes for human judgment in tasks such as report writing and evidence interpretation [12].

Many tools do not integrate the CKC and 5W1H models, which can improve the effectiveness of investigations by providing contextual and systematic analysis. The lack of automation, easy-to-use interfaces, and reporting capabilities leads to inefficiency, inaccuracy, and reduced adoption among forensic professionals. This gap highlights the need for flexible tools that automate digital forensic investigations by integrating the CKC and 5W1H frameworks. The CKC model, introduced by Lockheed Martin, is a crucial tool for mapping and analyzing cyber attacks. It provides a structured framework for understanding the stages of an attack, from initial reconnaissance to data exfiltration. The Digital Forensics Framework for Reviewing and Investigating cyber-attacks (D4I) enhances the examination and analysis phases of cyber-attack investigations, categorizing digital artifacts and mapping them to CKC steps [24]. This framework emphasizes the importance of structured examination and analysis processes, which are essential for effective cyber-attack investigations.

The primary objective of our research is to develop a comprehensive framework that automates digital forensic investigations while integrating analytical frameworks like the CKC and the 5W1H (Who, What, When, Where, Why, How) model. This framework aims to streamline the investigative process, providing detailed and structured insights into digital evidence. A key focus of this research is to analyze and identify behavioral patterns within digital forensic data, enabling investigators to understand attacker methodologies, predict potential attack vectors, and establish patterns of malicious activity across different incident cases. By examining behavioral patterns, the framework will help forensic analysts identify commonalities in attack strategies, recognize recurring threat actor signatures, and develop profiles of cybercriminal behavior that can enhance future investigations and threat intelligence.

These studies collectively demonstrate the potential of the 5W1H framework in enhancing the effectiveness and efficiency of information extraction in digital forensics. Our research has the potential to significantly impact the field of digital forensics by improving investigation outcomes, making resource use more efficient, and enhancing the ability to address complex cyber threats. By automating forensic processes and integrating frameworks like CKC and 5W1H, our framework streamlines investigations, providing detailed, structured insights that enhance accuracy and reliability. This framework benefits various stakeholders: forensic analysts gain a powerful, user-friendly resource for thorough investigations and behavioral pattern analysis; law enforcement agencies receive quicker, more precise evidence analysis with insights into criminal behavior patterns; and legal professionals obtain clear, comprehensive reports that strengthen legal proceedings. Ultimately, this innovation advances the effectiveness and efficiency of digital forensic investigations, contributing to stronger cyber defense and justice systems.

II. RESEARCH METHOD

This research uses a mixed-methods approach to develop a digital forensics framework that combines the D4I (Digital Forensics framework for Reviewing and Investigating cyber attacks) with the Cyber Kill Chain (CKC) and 5W1H models, enhanced with behavioral pattern analysis. The methodology consists of four main phases depicted in Fig.1. : (1) literature review to identify gaps in existing tools, (2) data collection from experimental scenarios, (3) framework development integrating D4I's artifact categorization and mapping approach with behavioral pattern recognition capabilities, and (4) validation through testing and comparison with existing methods. Data will be collected from controlled experimental environments using phishing attack scenarios specifically targeting the Kredivo application, including system logs, network traffic, application behavior, user interaction patterns, and digital artifacts generated during the simulated phishing attacks.

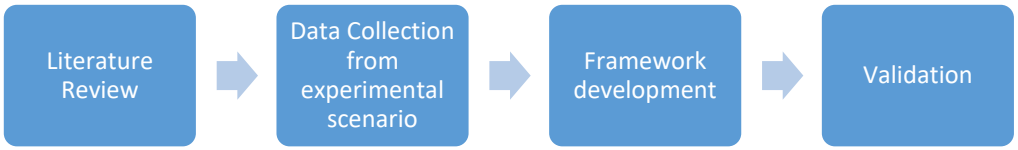

Fig.1. Research Method

Data collection was conducted through a simulated phishing attack on Kredivo fintech users in a controlled environment. The main objective of this process is to obtain digital artifacts that reflect the activity traces between the perpetrator and the victim, which are then used as the basis in the digital forensic investigation process. Two smartphone devices were used to simulate the victims: (1) iPhone 11 with iOS 15.8.1 operating system; (2) Vivo Y21 with Android 8.1.0 operating system. Data acquisition was performed using MOBILedit Forensic Express PRO (v7.4.0.20393). This application allows for data extraction from various sources, including WhatsApp messages, browser logs, file metadata, and OTP communications.

The IFIF framework as a proposed framework, which has seven main steps, was used to do the forensic analysis. During the Preparation & Collection phase, digital evidence is taken from victim devices, forensic images are made, and hash functions are used to check the integrity of the data. During the Attack Phase Mapping (CKC) stage, all the artifacts that were collected are sorted into the seven phases of the Cyber Kill Chain: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command & Control, and Actions on Objectives. The Artifact Identification & Correlation (D4I) stage uses the D4I method to sort artifacts into their CKC phases and make a Chain of Artifacts (CoA) that shows how the attack happened over time. We look at each artifact and attacker action in more depth by answering the questions of Who, What, When, Where, Why, and How through Contextual Analysis (5W1H). The Automation Tools phase uses tools like Python scripts to semi-automate tasks like parsing logs, extracting metadata, and adding 5W1H labels. The Behavioral Pattern Recognition stage finds patterns in the way attackers act and the strategies they use that happen over and over again. This helps to create a profile of the threat actor. Finally, in the Reporting & Visualization phase, the results are put together into a digital forensic report that is ready for court. This report includes CKC-phase visuals, Chain of Artifact (CoA) diagrams, and 5W1H summaries to help with clear communication and investigation.

The IFIF framework was proven to work in several important areas of forensic investigation. By mapping the discovered digital artifacts to the right parts of the CKC, it was able to find all the stages of the cyberattack. It also made it possible to build a logical and chronological CoA that told the story of what the attacker did. The framework used the 5W1H method to give full contextual explanations for each event, which made the investigation clearer. IFIF also made investigations go more smoothly by partially automating tasks like parsing logs and labeling artifacts. Lastly, the framework made well-organized, legal-ready forensic reports that digital forensic teams, law enforcement agencies, and lawyers could all use.

III. RESULTS AND DISCUSSION

A. Proposed Framework

The focus of the framework is on automation, integration of the Cyber Kill Chain (CKC) and 5W1H, as well as the need for efficiency in digital forensics investigations. Here is the recommended form of the framework called the Integrated Forensics Investigation Framework (IFIF). The main stages of the IFIF framework are (1) Preparation & Collection; (2) Attack Phase Mapping; (3) Artifact Identification & Correlation; (4) 5W1H-based Contextual Analysis; (5) Automation Engine; (6) Pattern Recognition; and (7) Reporting & Visualization. All explanations of the stages are shown in TABLE I.

TABLE I
PROPOSED FRAMEWORK IFIF

Phase	Description	Model
Preparation & Collection	Acquisition of digital evidence from the target device/system. Including imaging, hash verification, and documentation.	-
Attack Phase Mapping	Classify each digital artifact into the 7 phases of CKC (Recon, Weaponization	Cyber Kill Chain
Artifact Identification & Correlation	Use the D4I method to identify artifacts (logs, OTP, links, form submissions, etc.) and build a Chain of Artifacts (CoA).	D4I + CKC
5W1H Based Contextual Analysis	Use the 5W1H questions for each phase of CKC to understand the context of the attack. For example: Who sent the link? What was exploited?	5W1H
Automation Engine	Use a tool that can perform automatic log parsing, CKC mapping, and artifact extraction with natural language labeling for 5W1H.	LLM
Pattern Recognition	Analysis of the perpetrator's behavior patterns from artifacts: domain reuse, attack timing, C2 methods, etc. Create a threat actor profile.	Behavioral analysis
Reporting & Visualization	Create a digital investigation report in standard legal format (chain of custody, evidentiary table, 5W1H summary). Visualization of CKC flow and connections between artifacts.	Legal-ready output

B. Data Collection and Validation

The CKC framework showed a detailed map of the phishing attack in the experimental results. During the reconnaissance phase, attackers looked at how users acted, their contact information, and the layout of the official Kredivo website to learn more about potential victims. In the "weaponization" phase, attackers used this information to make fake websites and phishing emails that looked a lot like Kredivo's official platform. These materials were made using social engineering to get people to give up personal information like WhatsApp numbers, ID cards, and email addresses.

During the delivery phase, phishing emails were sent through trusted channels like email or text messages. To get more people to click on the links, the emails often used urgency or attractive offers. When victims clicked the link, they were sent to the fake site, which started the "exploitation" phase. Here, the attackers stole private information by taking advantage of the victims' trust in how the site looked. Also, malicious scripts or disguised downloads let malware be installed on victims' devices without their knowledge.

After the data was stolen, the command and control (C2) infrastructure let attackers control the stolen information and infected devices from a distance. This infrastructure made it possible to monitor things in real time, add more malware, and make strategic changes. Finally, in the action on objectives phase, the attackers used the stolen credentials and personal information to make illegal purchases, steal identities, or launch more attacks. In some cases, the stolen data was sold on the dark web, which meant that the phishing operation was a complete success.

This study uses a mathematical model based on [24] to show how the phishing attack process works in a systematic way. The attack sequence is set up as a linear function of seven main CKC phases. Each phase F_i has one or more digital artifacts a_{ij} that show specific forensic actions that were seen during the event. Then, these artifacts are put together in a CoA to show the attack's chronological and logical progression, which is shown as:

$$\mathrm{CoA} = \langle a_{r1} \rightarrow a_{w1}, a_{w2}, a_{w3} \rightarrow a_{d1}, a_{d2} \rightarrow a_{e1}, a_{e2}, a_{e3} \rightarrow a_{i1} \rightarrow a_{c1}, a_{c2} \rightarrow a_{a1}, a_{a2} \rangle \quad (1)$$

This math model makes it easy to put together the whole attack lifecycle and find links between forensic artifacts at different stages. It makes the investigation easier by letting forensic analysts follow each step exactly, and it also provides a basis for making structured, court-admissible reports. This model also supports partial automation, which means that systems can automatically link artifacts to CKC phases and put together a coherent CoA for more in-depth analysis.

CoA={Number WA Target→Domain Phishing, SSL Certificate, WA Blast Engine→ Phishing Link WA Message Text→ Form Input (Email, NIK), OTP, Password→ Logger Script→ C2 Panel, Victim Log→ Kredivo Login Access, Illegal Transaction}

TABLE II
CKC INTEGRATE TO 5W1H

Phase	Category	Finding	CoA	5W1H
R	Target data	List of whatsapp number	Source	How
W	Tool	Smartphone, engine whatsapp blast, domain, dns server, SSl, programming, port 80	How to create media	How
D	Media	Whatsapp platform	How to communicate	Where
E	Target information	Data, password app, OTP	Data breach	What
I	Method	Link phishing	How to breach	When
C2	Control	Monitoring target activity	Response from target	Who
A	Attack type	Acquisition app access	Objective	Why

TABLE II shows the integration between the stages of the CKC and the 5W1H model to systematically analyze attacks based on the categories of artifacts found, the correlation between artifacts (CoA), and critical questions. Each phase of the CKC has specific categories, such as Reconnaissance (R) which focuses on collecting target data like WhatsApp number lists, with the question "How" to understand the data collection methods. The next phase, such as Weaponization (W), records the tools used, such as smartphones or DNS servers, and answers how the attack media is created. The Delivery (D) and Exploitation (E) phases explore the target's communication and information media, including data breach methods. In the Installation (I) phase, methods such as phishing links are used, while Command-and-Control (C2) involves monitoring the target's activities, answering "Who" is responsible for the response. The final phase, Actions on Objectives (A), explains the goals of the attack, such as gaining application access, with the question "Why."

Heatmap illustrates in Fig. 2. the intensity and distribution of attacker activities across the CKC phases, using color gradients to represent activity levels and a grid layout to show specific task distribution. The legend and summary provide quick interpretation of the visual data. From the visualization, it is evident that the Reconnaissance (R) phase contains the highest concentration of activity with four distinct actions, followed by the Weaponization (W) and Exploitation (E) phases, each with three activities. The remaining phases—Delivery, Installation, Command and Control (C2), and Actions on Objectives—each contain one activity. This visual representation helps investigators easily identify which phases are most active and supports pattern analysis within the D4I forensic framework.

Fig. 2. Visualization of activity and intensity

Fig. 3. Heatmap distribution

The heatmap shows in Fig. 3. where and how often attackers were active during the Cyber Kill Chain (CKC) phases. It also shows important actions that were taken during a fake phishing attack on Kredivo users. The gradient of blue from light to dark shows how active something is, and the black dots show specific pieces of evidence. The Reconnaissance (R) phase has the most activity, which includes things like setting up ports, SSL, DNS, and programming. The Weaponization (W) phase is also very active, with the creation of phishing domains, WhatsApp blasting engines, and infrastructure that supports these activities through smartphones. The Exploitation (E) phase is just as important because it is when user credentials like OTPs, passwords, and

personal information are stolen. The last four phases—Delivery (D), Installation (I), Command and Control (C), and Actions on Objectives (A)—have fewer but still important actions, like executing phishing links, keeping an eye on victims, and getting into the Kredivo account without permission. This visual mapping helps investigators find high-risk phases, figure out how the attacker works, and use D4I forensic analysis correctly.

If the framework fails to answer one of the 5W1H questions, an error analysis can be conducted to identify the cause and solution. For example, the failure to answer "Who" might be caused by a lack of information in the logs or the use of masking techniques by the attacker, which can be addressed by integrating additional data or analyzing behavioral patterns. If "What" is unanswered, the cause could be an unsupported data format or corrupted artifacts, necessitating solutions such as upgrading framework libraries and analysis modules. The absence of a timestamp can cause a failure to answer "When," which can be addressed by time normalization or correlating with other log sources. For "Where," geolocation issues can be resolved using offline databases or network path tracking methods. If the framework cannot answer "Why," the use of AI for inferring motivation or enriching the dataset may be needed. Finally, the failure to answer "How" can be addressed by updating the exploitation library or conducting dynamic analysis on the artifacts. Each error must be recorded, and the framework should be continuously improved based on these findings to ensure analytical capability.

The IFIF framework worked well in the case study for fully mapping cyberattacks according to the Cyber Kill Chain phases. By combining the Chain of Artifacts (CoA) and the 5W1H contextual approach, it showed that it could build strong investigative narratives. The framework was also flexible enough to work with partial automation and modern forensic tools, which made it useful for real-world investigations in the fintech field and beyond. Based on these results, IFIF looks like a promising new way to use a structured and context-aware framework to automate digital forensic investigations.

B. Benchmarking Analysis

To evaluate the proposed framework's effectiveness, a qualitative benchmarking was conducted by comparing its features with Autopsy and the D4I. Autopsy is a widely used open-source tool that excels in data collection and artifact extraction, while D4I focuses on structured analysis based on the CKC.

TABLE III
RESULT OF BENCHMARKING ANALYSIS

Feature	Autopsy	D4I	IFIF
Artifact Collection	available	No artifact	Available via autopsy integration
CKC Mapping	Not available	available	Available
5W1H Contextual Analysis	Not available	Not available	Available
Automation of Investigation	Limited	Moderate	High
Report Visualization	Basic	Moderate	Advanced (via JSON and diagram)
Case Study Tested	General use	Synthetic scenario	Phishing Kredivo case

To obtain the benchmarking results as shown in TABLE III, a qualitative evaluation was conducted on three approaches, namely Autopsy, D4I Framework, and the proposed IFIF framework.The assessment was conducted based on six important criteria in the automation of digital forensic investigations, including the ability to collect artifacts, mapping into the CKC, 5W1H-based contextual analysis, level of automation, report visualization, and the case studies used.

In the aspect of artifact collection, Autopsy has strong capabilities, while D4I does not explicitly manage artifacts, and the IFIF framework relies on integration with Autopsy for this stage.In terms of CKC mapping, Autopsy does not provide this feature, unlike D4I and the proposed framework which are capable of systematically mapping artifacts to the CKC phases.In the context of 5W1H analysis, neither Autopsy nor D4I

supports contextual question-based analysis, whereas the IFIF framework enriches investigations by answering the questions "Who," "What," "When," "Where," "Why," and "How" for each artifact.

The level of investigation automation in Autopsy is considered limited because it still requires a lot of manual intervention, whereas D4I offers moderate automation, and the IFIF framework achieves a high level of automation thanks to the Python Flask-based pipeline and JSON output. From the perspective of report visualization, Autopsy only produces text-based reports, D4I provides moderate visualization, while IFIF offers advanced visualization through artifact diagrams and IFIF artifact integration. Lastly, for validation through case studies, Autopsy was applied for general use, D4I was tested in synthetic scenarios, while the IFIF framework was tested through real phishing scenarios on the Kredivo application, demonstrating its practical relevance to modern cyber threats.

C. Discussion

In order to improve investigative results, recent advancements in digital forensics have placed a greater emphasis on combining partial automation, context-aware reasoning, and structured modeling. Dunsin et al. [25] examined AI applications for threat pattern detection and evidence classification, while Wickramasekara et al. [26] showed how large language models (LLMs) could automate log parsing and artifact labeling. The SANS DFIR trends for 2024 [27] also showed an increasing dependence on automated triage and cloud/mobile evidence. ForensiCross, a blockchain-based solution for preserving evidence integrity in dispersed environments, was concurrently proposed by Akbarfam et al. [28]. A 2024 systematic review of structured attack analysis [29] emphasized the role of artificial intelligence in the Cyber Kill Chain (CKC), particularly in improving detection capabilities across attack stages and modeling adversarial behavior..

More precisely, the significance of situation awareness and contextual knowledge in digital investigations has been covered in a number of recent studies. In order to close the gaps between technical findings and legal interpretation, Han, Kim, and Lee [30] proposed a 5W1H-based expression model that formalizes forensic information sharing using natural question structures. In order to provide situational clarity during investigations, Ferrante and Habibnia [31] proposed a technique for directly extracting and responding to 5W questions from forensic artifacts and system metadata. In order to improve situation awareness and decision-making in intricate investigation scenarios, Grigaliūnas et al. [32] developed the Digital Evidence Object Model (DEOM), which organizes digital artifacts as context-rich entities.

These studies tend to concentrate on post-collection stages like documentation, explanation, and human decision support, even though they make a substantial contribution to forensic reasoning and interpretation. However, the IFIF (Integrated Forensic Investigation Framework) suggested in this study offers a more comprehensive solution by combining contextual reasoning (5W1H), artifact correlation (through D4I), and CKC-based attack mapping into a single structured workflow, which is further enhanced by partial automation for repetitive tasks like log parsing and artifact tagging. In order to help analysts and legal stakeholders comprehend the incident, IFIF not only maps technical traces but also explains the reasoning behind each stage of the attack. To set itself apart from earlier methods, the framework additionally facilitates cross-phase visualization, legal-ready reporting, and behavioral profiling.

IV. CONCLUSION

This research contributes to digital forensics automation based on the integration of CKC and the 5W1H model, which enables systematic analysis of each stage of an attack by answering critical questions such as "Who," "What," and "How." This framework provides a structured approach that facilitates investigations, especially on large and complex datasets, and enhances accuracy in identifying attack patterns and correlations between artifacts. The potential for its application in the real world is immense, such as in investigating

cybersecurity incidents in organizations, threat analysis on cloud service providers, and the development of automated security systems that can detect and mitigate attacks in real-time.

The novelty of this work lies in the integration of CKC and 5W1H frameworks in a semi automated, web-based forensic investigation tool. Unlike existing approaches, our framework provides structured artifact chaining, contextual analysis, and advanced visualization, enabling investigators to efficiently process complex cyber attack cases such as phishing. For future research, this framework can be integrated with more advanced AI technologies, such as deep learning for attack prediction and more complex pattern recognition. In addition, implementation on an industrial scale, including in the financial, government, and manufacturing sectors, can expand the scope and relevance of the framework in addressing the increasingly evolving cyber security threats. To support reproducibility, the implementation scripts along with simulated phishing case data are openly accessible via GitHub at: https://github.com/totoraha/totoraha-d4i-forensics.

REFERENCES

[1] A. Asasfeh, N. A. Al-Dmour, H. Al Hamadi, W. Mansoor, and T. M. Ghazal, "Exploring Cyber Investigators: An In-Depth Examination of the Field of Digital Forensics," in 2023 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), 2023, pp. 84–88. doi: 10.1109/DASC/PiCom/CBDCom/Cy59711.2023.10361449.

[2] N. A. Rakha, "Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations," Mex. Law Rev., 2024, doi: 10.22201/iij.24485306e.2024.2.18892.

[3] G. Shukla, "Cyber crime investigation and digital forensics," SSRN Electronic Journal, 2023, doi: https://doi.org/10.2139/ssrn.4616519.

[4] A. Ombu, "Role of Digital Forensics in Combating Financial Crimes in the Computer Era," Journal of Forensic Accounting Profession, vol. 3, no. 1, pp. 57–75, Jun. 2023, doi: https://doi.org/10.2478/jfap-2023-0003.

[5] G. Michelet, F. Breitinger, and G. Horsman, "Automation for Digital Forensics: Towards a definition for the community," Forensic Science International, vol. 349, pp. 111769–111769, Jun. 2023, doi: https://doi.org/10.1016/j.forsciint.2023.111769.

[6] G. Michelet, F. Breitinger, and G. Horsman, "Automation for digital forensics: Towards a definition for the community.," Forensic Sci. Int., vol. 349, p. 111769, Aug. 2023, doi: 10.1016/j.forsciint.2023.111769.

[7] M. Matijević Gostojić and Ž. Vuković, "A knowledge-based system for supporting the soundness of digital forensic investigations," Forensic Science International: Digital Investigation, vol. 46, p. 301601, Sep. 2023, doi: https://doi.org/10.1016/j.fsidi.2023.301601.

[8] B. G. Bokolo and Q. Liu, "Artificial Intelligence in Social Media Forensics: A Comprehensive Survey and Analysis," Electronics, vol. 13, no. 9, p. 1671, Jan. 2024, doi: https://doi.org/10.3390/electronics13091671.

[9] John Sitima, "Understanding Digital Forensic Tools: Their Features, Applicability and Key Short Comings. A Compendium," International Journal For Multidisciplinary Research, vol. 6, no. 6, Nov. 2024, doi: https://doi.org/10.36948/ijfmr.2024.v06i06.30026.

[10] W. Neuteboom, A. Ross, L. Bugeja, S. Willis, C. Roux, and K. Lothridge, "Quality Management in forensic science: A closer inspection," Forensic Science International, vol. 358, p. 111779, Jul. 2023, doi: https://doi.org/10.1016/j.forsciint.2023.111779.

[11] J.-A. Patteet and C. Champod, "Striated toolmarks comparison and reporting methods: Review and perspectives," Forensic Science International, vol. 357, p. 111997, Apr. 2024, doi: https://doi.org/10.1016/j.forsciint.2024.111997.

[12] A. Wickramasekara, F. Breitinger, and M. Scanlon, "Exploring the Potential of Large Language Models for Improving Digital Forensic Investigation Efficiency," arXiv (Cornell University), Feb. 2024, doi: https://doi.org/10.48550/arxiv.2402.19366.

[13] Amy Arabella Singh and M. Okpeku, "EMERGING METHODS OF HUMAN MICROBIOME ANALYSIS AND ITS FORENSIC APPLICATIONS: Reviews," Forensic science international. Reports, vol. 9, pp. 100355–100355, Jul. 2024, doi: https://doi.org/10.1016/j.fsir.2024.100355.
[14] J. Finnis et al., "Illuminating the benefits and limitations of forensic light sources," Science & Justice, vol. 63, no. 1, pp. 127–134, Jan. 2023, doi: https://doi.org/10.1016/j.scijus.2022.12.001.
[15] A. Khare, "Converging Vulnerability Insights: Unifying Vulnerability Intelligence For Enhanced Application Security With Collaboration," 2024 ITU Kaleidoscope: Innovation and Digital Transformation for a Sustainable World (ITU K), pp. 1–8, Oct. 2024, doi: https://doi.org/10.23919/ituk62727.2024.10772872.
[16] X. Chango, O. Flor-Unda, P. Gil-Jiménez, and H. Gómez-Moreno, "Technology in Forensic Sciences: Innovation and Precision," Technologies, vol. 12, no. 8, pp. 120–120, Jul. 2024, doi: https://doi.org/10.3390/technologies12080120.
[17] Larassaty Chandra Pakaya and Imam Riadi, "Forensic Analysis of Web-based Instant Messenger Applications using National Institute of Justice Method," International Journal of Computer Applications, vol. 185, no. 35, pp. 44–51, Sep. 2023, doi: https://doi.org/10.5120/ijca2023923145.
[18] F. Abu, Mahmmoud Jazzar, Amna Eleyan, and Tarek Bejaoui, "Forensics Investigation on Social Media Apps and Web Apps Messaging in Android Smartphone," vol. 90, pp. 1–7, Jul. 2023, doi: https://doi.org/10.1109/smartnets58706.2023.10216267.
[19] Omego Nnamonu, M. Hammoudeh, and Tooska Dargahi, "Digital Forensic Investigation of Web-Based Virtual Reality Worlds: Decentraland as a Case Study," IEEE Communications Magazine, vol. 61, no. 9, pp. 72–78, Sep. 2023, doi: https://doi.org/10.1109/mcom.005.2200688.
[20] Ganesh Majeti, Sai Sundar YVL, Sai Shanmukh Ulichi, Sachi Nandan Mohanty, and S. V. Sudha, "Digital Forensic Advanced Evidence Collection and Analysis of Web Browser Activity," ICST Transactions on Scalable Information Systems, Jun. 2023, doi: https://doi.org/10.4108/eetsis.3357.
[21] A. Khare, "Converging Vulnerability Insights: Unifying Vulnerability Intelligence For Enhanced Application Security With Collaboration," 2024 ITU Kaleidoscope: Innovation and Digital Transformation for a Sustainable World (ITU K), pp. 1–8, Oct. 2024, doi: https://doi.org/10.23919/ituk62727.2024.10772872.
[22] Dr. K. V. K. Santhy and Dr. A. S. Padmanabhan, "A Review on the Changing Dimensions of Digital Forensics in Criminal Investigations," SSRN Electronic Journal, 2023, doi: https://doi.org/10.2139/ssrn.4329086.
[23] S. S. Alqahtany and T. A. Syed, "ForensicTransMonitor: A Comprehensive Blockchain Approach to Reinvent Digital Forensics and Evidence Management," Information, vol. 15, no. 2, p. 109, Feb. 2024, doi: https://doi.org/10.3390/info15020109.
[24] A. Dimitriadis, E. Lontzetidis, B. Kulvatunyou, N. Ivezic, D. Gritzalis, and I. Mavridis, "Fronesis: Digital Forensics-Based Early Detection of Ongoing Cyber-Attacks," IEEE Access, vol. 11, pp. 728–743, 2023, doi: https://doi.org/10.1109/access.2022.3233404.
[25] D. Dunsin, M. C. Ghanem, K. Ouazzane, and V. Vassilev, "A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response," Forensic Science International: Digital Investigation, vol. 48, no. 301675, p. 301675, Mar. 2024, doi: https://doi.org/10.1016/j.fsidi.2023.301675.
[26] A. Wickramasekara, F. Breitinger, and M. Scanlon, "Exploring the potential of large language models for improving digital forensic investigation efficiency," Forensic Science International: Digital Investigation, vol. 52, p. 301859, Feb. 2025, doi: https://doi.org/10.1016/j.fsidi.2024.301859.
[27] "Advanced Evidence Collection: DFIR's 2024 Mobile and Cloud Shift | SANS Institute," Sans.org, Oct. 04, 2024. https://www.sans.org/blog/advanced-evidence-collection-dfir-s-2024-mobile-and-cloud-shift/
[28] Akbarfam, Asma Jodeiri, G. Dorai, and H. Maleki, "Secure Cross-Chain Provenance for Digital Forensics Collaboration," arXiv (Cornell University), Jun. 2024, doi: https://doi.org/10.48550/arxiv.2406.11729.
[29] M. Kazimierczak, N. Habib, J. H. Chan, and T. Thanapattheerakul, "Impact of AI on the Cyber Kill Chain: A Systematic Review," Heliyon, p. e40699, Dec. 2024, doi: https://doi.org/10.1016/j.heliyon.2024.e40699.
[30] J. Han, J. Kim, and S. Lee, "5W1H-based Expression for the Effective Sharing of Information in Digital Forensic Investigations," arXiv (Cornell University), Jan. 2020, doi: https://doi.org/10.48550/arxiv.2010.15711.

[31] C. Ferrante and Babak Habibnia, “Answering to 5W Using Digital Forensics Data,” Nov. 2021, doi: https://doi.org/10.1109/iscsic54682.2021.00043.
[32] S. Grigaliunas, J. Toldinas, A. Venckauskas, N. Morkevicius, and R. Damasevicius, “Digital Evidence Object Model for Situation Awareness and Decision Making in Digital Forensics Investigation,” IEEE Intelligent Systems, pp. 1–1, 2020, doi: https://doi.org/10.1109/mis.2020.3020008.