International Journal Software Engineering and Computer Science (IJSECS)
5 (2), 2025, 560-575
Published Online August 2025 in IJSECS (http://www.journal.lembagakita.org/index.php/ijsecs)
P-ISSN: 2776-4869, E-ISSN: 2776-3242. DOI: https://doi.org/10.35870/ijsecs.v5i2.4371.

RESEARCH ARTICLE Open Access

Opportunities and Challenges of Artificial Intelligence in Digital Forensics

Syifaurachman *
Department of Information Systems, Faculty of Computer Science, Universitas Pamulang, South Tangerang City, Banten Province, Indonesia.
Corresponding Email: dosen03181@unpam.ac.id.

Received: May 28, 2025; Accepted: June 30, 2025; Published: August 1, 2025.

Abstract: Digital forensics research remains constrained, while the rapidly evolving digital landscape renders traditional forensic methodologies increasingly inadequate for modern investigative challenges. This work conducts a systematic literature review and bibliometric analysis of computer forensics, specifically targeting digital forensics applications. The study employed a systematic literature evaluation of the Scopus database using "Computer Forensic" as the search term within article titles, abstracts, and keywords. The initial search retrieved 3,222 publications, subsequently refined to 120 academic articles through PRISMA methodology with inclusion criteria encompassing computer science subject areas, final journal articles, English language publications, and open access availability. Three research questions guide this investigation: examining future digital forensic research directions, analyzing current research methodologies, and identifying practical and theoretical implications. Data collection occurred on May 21, 2025, with analysis performed using VOS Viewer bibliometric software. Results reveal that digital forensics research predominantly originates from industrialized nations, particularly the United States and Europe, accounting for 49 of 120 examined articles (40.83%), while Asian and African contributions remain substantially underrepresented. The analysis identified a four-stage digital forensics implementation framework: identification, collection, analysis, and preservation. Furthermore, the investigation examined artificial intelligence applications in digital forensics, particularly NLP-based approaches and machine learning algorithms including CNN models for forensic processes. While AI has revolutionized digital forensics by enhancing accuracy, efficiency, and investigative effectiveness, the analysis reveals persistent challenges including algorithmic bias, data privacy concerns, and decision-making transparency issues. Future research should incorporate additional databases such as Web of Science to enhance data quality and scope. The integration of AI and machine learning models across digital forensics stages promises to deliver more precise and thorough investigative outcomes.

Keywords: Computer Forensics; Digital Forensics; Literature Review; Artificial Intelligence.

1. Introduction

The growing complexity of cyber threats, combined with the rapid proliferation of digital ecosystems, has had a significant impact on the field of digital forensics. Traditional forensic processes frequently fail to satisfy the demands of this evolving environment [1][2]. The implementation of artificial intelligence (AI) into digital forensics has emerged as a game changer, propelling computer forensic research to the forefront of technological innovation. AI-powered approaches, such as machine learning, natural language processing, and image and video analysis, have greatly improved the accuracy, efficiency, and speed of forensic investigations. These technologies enable large-scale data analysis, streamline investigative operations, and reveal intricate digital patterns, ultimately boosting case resolution and evidence interpretation. However, the deployment of

AI creates significant obstacles, including ethical questions about privacy, algorithmic bias, and the admissibility of AI-generated evidence in court proceedings. This research approaches a systematic literature review (SLR) with PRISMA method is therefore required to synthesize knowledge, identify current gaps, and aid in the development of sophisticated forensic procedures. One of the key goals for performing an SLR is to incorporate ethical considerations into forensic procedures. Ethical flaws in digital investigations might jeopardize the quality and credibility of forensic findings. Systematic reviews offer a formal platform for analyzing existing frameworks and integrating ethical principles into digital forensic readiness [3][4]. Furthermore, there is a growing demand for proactive forensic skills. Real-time response and automated forensic procedures are underrepresented in the current literature, emphasizing the significance of conducting systematic reviews when constructing such models. These evaluations allow researchers to completely map digital forensic processes, hence facilitating framework development targeted to evolving risks and technology [5].

Systematic reviews also help to gain a better understanding of specialized subfields, such as memory forensics and user attribution. For example, information from volatile memory forensics studies inform how transient data is handled throughout investigations. Similarly, assessments that assess the effectiveness and limitations of behavior-based user attribution, an area confronting issues in suspect identification, enhance this field [6]. Furthermore, the integration of artificial intelligence (AI) into digital forensics is a promising trend. AI-enhanced techniques provide more efficient and accurate analysis of digital evidence. Systematic reviews can evaluate existing AI applications, identify limitations, and propose future implementation strategies [7]. In conclusion, a comprehensive literature evaluation in the field of digital forensics is both timely and important. It promotes the creation of ethical, adaptable, and forward-thinking forensic frameworks, assures alignment with technological improvements, and improves investigative efficacy.

The formalization of digital forensic requirements, including legal and evidential standards, is a promising trend [8]. An SLR contributes not just by tracking these advances, but also by encouraging transparency and rigor in the synthesis of existing evidence [9]. Without such assessments, discipline risks fragmented growth and the continuation of unsolved issues, hurting both investigative accuracy and the advancement of forensic science. The need for a literature review in the field of computer and digital forensics stems from both technological and methodological improvements. The advent of anti-forensic techniques and the push for automation in real investigations need fresh tools and processes that are usually scattered over several studies [10]. Moreover, as digital ecosystems become increasingly interconnected, traditional forensic methods struggle to keep pace, signaling a paradigm shift that necessitates a comprehensive reassessment of current capabilities [11]. Ethical integrity remains another pressing concern. The absence of a standardized ethical code may compromise the reliability of forensic outcomes, emphasizing the need for SLRs to help formulate and validate ethical frameworks [12]. However, conducting an SLR in this domain is not without challenges—many existing reviews are limited to technical evaluations and overlook ethical dimensions, while issues such as organizational barriers and human error introduce inconsistencies.

This study aims to investigate the current landscape of Islamic leadership research and assess the topic's continued relevance as a target for future research. This study also examines the evolution of academic discourse on Islamic leadership and seeks to determine how this work might be applied to leadership theories and organizational practices. The research questions posed include:

RQ1 : *Is the exploration of digital forensics a subject that continues to hold significance for future scholarly inquiry?*
RQ2 : *How are research investigations into digital forensics?*
RQ3 : *What are the practical as well as theoretical implications for future research?*

This study addresses the three research issues through a Systematic Literature Review (SLR) and Bibliometric Analysis. The systematic literature review method is excellent for summarizing existing research and identifying gaps, trends, and future study paths, as well as giving evidence-based insights that may be used to affect policy, practice, and research. This ensures that findings are obtained from a diverse and representative sample of studies while also highlighting topics for additional investigation. The bibliometric study will supplement the review by assessing the distribution and impact of publications about computer forensic focus on area digital forensics. Using VOS Viewer and the Scopus database, this study will examine computer forensic publications from various journals, with an emphasis on articles published up to May 21, 2025. This methodology allows for a detailed mapping of the field's evolution and provides a thorough grasp of future research opportunities and challenges.

2. Related Work

2.1 Concept of Digital Forensic

Digital forensics is the scientific use of methods and ideas to identify, acquire, examine, and analyze digital data. This procedure must ensure that the information's integrity is constantly maintained and that a strict chain of custody is followed throughout the investigation. By adhering to these standards, digital forensic practitioners can guarantee that the evidence remains credible and admissible in legal and investigative contexts proposed a mechanism for distributing meta-information related to a system's principles for digital forensic investigations. This allows for the analysis of events in a system and the collection of more evidence [13]. Digital forensics is a specialized area with an emphasis on the investigation, analysis, and preservation of digital evidence, especially within the contexts of developing technologies like blockchain and cloud computing, the proposed framework plays a vital role in strengthening data integrity and authenticity within digital forensic investigations, thereby ensuring the reliability of the collected evidence [14]. Digital forensics is an area of forensic science that deals with the extraction, processing, and evaluation of digital artifacts obtained from various electronic devices. Its significance has grown exponentially as society has become increasingly reliant on digital technologies and processes. File carving is one of the methodologies employed in this discipline, which enables the recovery of deleted or corrupted data by analyzing raw binary information that is independent of the file system's metadata. Accurate classification of file fragments is an important component of this procedure since it allows for effective reconstruction of fragmented files. This capacity is critical for successful data recovery and plays an important role in forensic investigations. This study concentrates on the classification of file fragment types within the domain of digital forensics, a task critical to the accurate reconstruction of digital evidence. To address this challenge, the paper introduces lightweight convolutional neural network (CNN) models that utilize depth wise separable convolutions an efficient architectural design aimed at minimizing computational complexity [15]. The proposed digital forensic framework, "Crime Detection and Diminution in Digital Forensics (CD3F)," is made up of eight key workflow stages: forensic request, preparation, examination, identification, collection, analysis, acquisition, and forensic reporting. These stages help to plan and lead the entire digital forensic investigation process. CD3F is designed to be technology-neutral, with broad applicability across forensic cases and research platforms, allowing investigators to adapt the framework to a variety of situations. The major goal of CD3F is to improve the effectiveness and efficiency of investigations by offering a systematic approach to both crime detection and prevention. Although promising, the paradigm requires additional validation through real-world implementation in case studies [16].

2.2 Digital Forensic using AI-Based

Explain digital forensics as an interdisciplinary area that includes the systematic gathering, analysis, interpretation, and presentation of digital evidence gathered from a variety of electronic devices. This domain incorporates fundamental knowledge and approaches from other disciplines, including computer science, criminology, and law, to support investigative and judicial procedures. The collaborative nature of digital forensics ensures that both the technical and legal aspects of digital evidence are addressed, thereby improving the reliability and admissibility of findings in formal proceedings. In the study of a digital forensic technique using NLP tools for investigations, two individuals, Eva and Bob, were identified as persons of interest in the context of a forensic investigation. To examine text generated by large language models (LLMs), natural language processing (NLP) techniques were used, allowing for a deeper investigation of linguistic patterns and content. However, this study has not yet given validity of the findings through a greater scale of data and is solely based on text data, the researcher acknowledges that in the future, data other than text, such as audio, would be required to enable more accurate analysis [17]. The digital forensics process typically involves three fundamental phases: the collection, preservation, and analysis of digital evidence, all of which are essential for conducting thorough and effective investigations into unlawful activities and anti-competitive behavior. To enhance the efficiency and relevance of forensic procedures, digital forensic tools and applications can be categorized according to various criteria, including their primary function, the type of device they are designed for, the operating system they support, and their licensing model. This classification enables investigators to select and apply tools that are best suited to the specific context and requirements of each investigation. This research proposed architecture enhances digital forensics applications' efficiency with method used Digital forensics tools for data extraction and analysis are utilized and AI-based applications process large datasets automatically [18]. The work describes a novel system for ranking questionable artifacts in the field of digital forensics. The suggested approach uses artificial intelligence to improve the efficiency and precision of detecting malicious digital artifacts. A dual-validation approach is used to improve anomaly detection and reduce the number of false positives. Empirical evaluations show that the system is very accurate in distinguishing between innocuous and malicious artifacts, highlighting its potential application in real-world

forensic investigations. However, this work has limitations in the validation of the tests carried out due to the dataset's secrecy limits and ignoring basic aspects of digital artifacts such as metadata and timestamps [19].

The study presents an AI-powered agent for cloud evidence collecting, solving critical difficulties such as protecting volatile data and maintaining the chain of custody. The system uses a blockchain paradigm to secure data integrity and provenance, which improves trustworthiness in digital evidence management. Future study hopes to build on this work by creating a web-based cloud forensics tool that will make forensic investigations in cloud systems more accessible and effective. The system uses AI agents to minimize the size of the evidence repository, increasing storage efficiency by only saving important data. This strategy also increases the trustworthiness of the chain of custody in cloud forensic investigations. Operating at the hypervisor level, the technology ensures robust and dependable evidence collection. The proposed AI agent enhances categorization accuracy inside cloud forensics. However, this research is limited to memory evidence acquisition, emphasizing the significance of improving capacities to cover other types of digital evidence [20].

The study presents the Digital Trace Inspector (DTI), a tool for temporal metadata analysis in digital forensics with use two datasets were created using Windows 10 workstations to help evaluate the Digital Trace Inspector (DTI). These datasets include training dataset 1 and test dataset 1, which were created to imitate real-world user activity patterns. Metadata traces were retrieved from the systems using "PlasoLog2Timeline", a popular tool for creating forensic timelines. Each dataset was then divided into ten separate scenarios based on recorded datetime values, enabling detailed temporal analysis of digital footprints. DTI uses a Learning Classifier System to successfully assess user activity patterns, allowing for the detection of behavioral traces across time. The experimental results show the system's outstanding performance, with a high recall and an impressive average F1 score of 0.98, suggesting its durability and reliability in forensic investigations. However, the challenge is the availability of expert-labeled training data, which is required for validating rules and developing machine learning models, limiting the overall effectiveness of the system, and resulting in ambiguity in some classes, which can lead to misclassification. Addressing these challenges is critical for increasing the accuracy and scalability of forensic systems that rely on expert-generated rule sets [21].

The study used the CIDDS-001 dataset to find anomalies. Other datasets mentioned in the article include NSW-NB15 and CICIDS2017, demonstrating the breadth of data sources used for analysis. Meanwhile, the SWaT dataset was included in the analysis but not used for evaluation or testing. The SMS-I tool is part of a digital forensics system designed to improve cyber-physical correlation, forensic investigations, and incident response in critical infrastructures. It analyzes multidimensional data using multiple AI approaches, with a focus on discovering temporal correlations between cyber and physical alarms. Supervised algorithms are used to forecast event probabilities based on these alerts, and correlation criteria are developed to investigate repeated alert patterns. The tool also makes it easier to examine mitigation strategies for reported incidents. Machine learning approaches such as incident probability prediction and association rule mining are also used to help in decision-making. Overall, these AI-based technologies allow for more accurate and thorough examination of attack evidence across several data dimensions. Although, it's difficult to detect complex attack patterns by combining physical and cyber events [22].

The study describes a novel ransomware triage strategy that uses Large Language Models (LLMs) and the Volatility framework to analyze memory dumps. Experimental results show that the approach is highly accurate at recognizing ransomware-related processes, considerably boosting the reliability of memory forensics. This approach not only improves triage speed but also provides detailed and interpretable explanations, boosting overall decision-making during digital forensic examinations. The method volGPT identifies ransomware processes with high accuracy. It also provides comprehensive explanations during ransomware triage. Memory forensics for fileless malware remains an area that is not fully addressed. The reliance on process names limits volGPT's analysis capabilities. Additionally, no experiments have been conducted on benign samples to assess the system's robustness [23].

2.3 Digital Forensic in malware investigation

The paper examines the role of malware forensics in the investigation of ransomware occurrences, highlighting its importance in identifying and mitigating such threats. As part of its analysis, the research presents a case study focused on the behavioral patterns of Onion ransomware, offering insights into how this specific type of malware operates. Through detailed examination, the study contributes to the development of forensic strategies for detecting, analyzing, and responding to ransomware attacks more effectively. This research defines malware forensics as a systematic approach to detecting, analyzing, and examining the properties of malicious software to identify the perpetrators of cyberattacks and uncover the underlying motives behind such incidents. It underscores the critical role of digital evidence logs in forensic investigations, while also acknowledging the challenges posed by data loss resulting from actions such as disk formatting or encryption mechanisms that can obscure valuable forensic information. Moreover, the study stresses the importance of accurately understanding the behavioral patterns and technical signatures of ransomware, as this knowledge is essential for enhancing both detection capabilities and incident response strategies in digital

forensic practice. However, despite its in-depth discussion on various facets of digital forensics, the paper does not explicitly differentiate between the definitions of digital forensics and computer forensics as separate or distinct domains [24].

Table 1. Definition element of Digital Forensic

No.	Defining element of digital forensic	Reference
1	Digital forensics is the application of science to the identification, acquisition, examination, and analysis of data while protecting its integrity and maintaining a strict chain of custody for the data.	[13]
2	Digital forensics, or computer forensics, is a systematic and rigorous procedure for investigating and preventing cybercrime. It entails the identification, collecting, analysis, and preservation of electronic evidence from various digital devices, such as computers, smartphones, and other storage media.	[14]
3	Digital forensics is a specialized field of forensic science that focuses on the identification, retrieval, and investigation of digital artifacts from a variety of electronic devices.	[15]
4	Digital forensics are primarily concerned with systematic collection, analysis, interpretation, and presentation of evidence obtained from digital devices.	[16]
5	Digital forensics is the analysis of digital evidence using computer-intensive operations like data collecting, data carving, document indexing, and picture processing.	[17]
6	An essential aspect of digital forensics involves the identification, examination, and investigation of malware characteristics. This process aims to uncover the origin of cyberattacks, identify the individuals or groups responsible, and gain insight into the underlying motives behind such malicious activities.	[24]
7	The practice of digital forensics encompasses a series of methodical procedures, including the acquisition, extraction, analysis, and preservation of digital data. These processes are carried out in a manner that upholds forensic integrity, guaranteeing that the evidence remains authentic and admissible in legal situations.	[25]

Table 1, summarizes the findings of this study's investigation of how several researchers create a cycle for doing digital forensics on the things they examine. Seven researchers who provided insights into what aspects or stages are involved in implementing digital forensics. This can be a very useful resource for understanding how a cycle is formed during the implementation stages of digital forensics.

3. Research Method

A systematic literature evaluation that uses a bibliometric approach systematically evaluates literature to identify trends, patterns, and major research entities within a topic. Using frameworks such as PRISMA, this technique enables a thorough and reproducible literature review, presenting a clear and transparent picture of the topic under consideration [26]. The following inclusion criteria were established: (1) works published before May 21, 2025, (2) publications in English, and (3) focusing on the topic of Computer Forensics with a specific subject area of Digital Forensics. Bibliometric analysis was carried out with VOS Viewer, which visualized bibliographic data to assess citation networks, author partnerships, and co-occurring keywords, exposing the intellectual structure and dynamics of the research area. The combination of bibliometric analysis with systematic review enables researchers to combine empirical data and map the landscape of research activity, including identifying significant contributors and emerging trends. The combination of both methodologies provides a thorough picture of the research field's evolution, historical flow, and future direction, making it extremely useful in interdisciplinary studies for gaining deeper insights. Bibliometric analysis is also employed strategically in scholarly publishing, evaluating scientific journals based on their economic weight. The initial phase in an academic study is to select keywords, which can be accomplished through a macro methodology (top-down), ranging from wide search trajectories to more narrowly targeted studies and themes. As a result, after considering the limitations of past research and the scarcity of studies on Computer Forensics, this study employs the keyword "Computer Forensic" as a main point in the article's title, abstract, and keywords sections. Furthermore, researchers utilize the Scopus database for a range of investigative purposes, such as conducting literature reviews, identifying subject matter experts, and monitoring research trends.

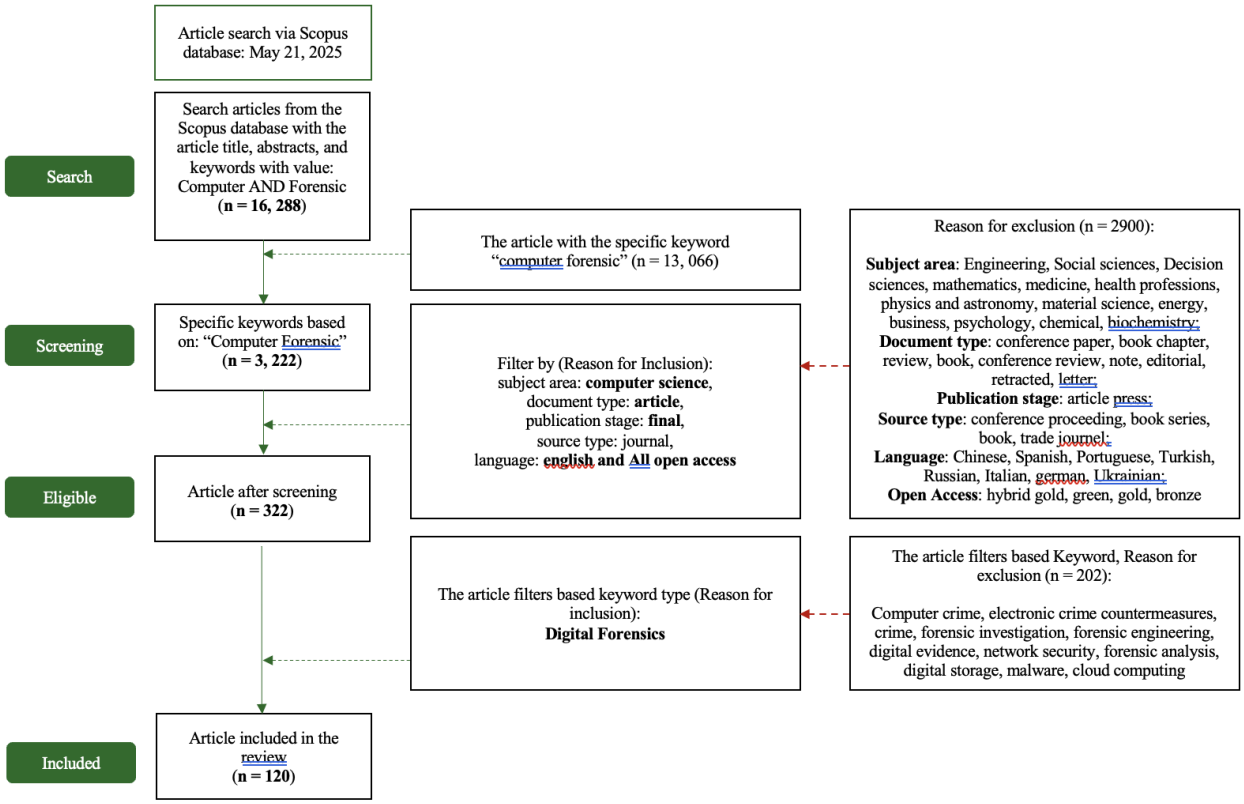


Figure 1. Systematic Literature Review information flow using PRISMA Model

According to the search results obtained on May 21, 2025, via the database of Scopus using the publication's title, abstract, and keywords: "computer AND forensic" across diverse academic disciplines, spanning from the earliest publication in 2007 to the most recent in 2025, the total number of articles about Computer Forensic is 16, 288 documents (refer to Figure 1). Following these findings, a screening procedure sorts documents based on their classification. Articles are classified using filters based on computer science as the subject area (n = 2, 781), article as the document type (n = 828), final status as the publication stage (n = 812), journal as the source type (n = 756), English as the language (n = 756), and open access as the limit (n = 322). The screening results for a certain term with Digital Forensics returned 120 articles. This study reviewed as many as 120 final documents from the filtering results because the research is focused on the field of computer science and digital forensics topics, so that the filter is the main factor for researchers to choose. In addition to the selection of journal types, the use of English in journal documents and open access criteria are considered to make it easier for researchers to access article documents and make it easier to review and understand. The limitation study only from the Scopus database collection. The information provided is further analyzed in this study to answer *RQ1: Is the exploration of digital forensics a subject that continues to hold significance for future scholarly inquiry? RQ2: How are research investigations into digital forensics? RQ3: What are the practical as well as theoretical implications for future research?*.

4. Result and Discussion

4.1 Results

The results of this study focus on findings from 120 articles in the Scopus database on Computer forensic focus on area digital forensics. This data is sourced from identifying the number of articles published, publications throughout the years, and journal sources. This study will also highlight the most influential elements especially in digital forensics, including the authors, affiliations, and the countries involved.

RQ1: Is the exploration of Computer forensic focus on area digital forensics a subject that continues to hold significance for future scholarly inquiry?

According to the data retrieved from the Scopus database, it has been ascertained that over four decades, scholarly work about Computer forensic focus on area digital forensics comprises 120 articles; this suggests that investigations into Computer forensic focus on area digital forensics remain comparatively scarce, as illustrated in Figure 1.

The exploration of Computer forensic focus on area digital forensics commenced its progressive development during the last decade, specifically start from 2019. The inaugural study was executed by Buchholz & Spafford, 2007 and was entitled "Run-time label propagation for forensic audit data", which signified the advent of the term now recognized as Computer forensic specially focus on area digital forensics. Currently, the development of research on Computer Forensics about digital forensics has begun to attract many researchers, the increase in the number of publications in the past 5 years until mid-2025, on average 10%-30% although graphically there is fluctuation.

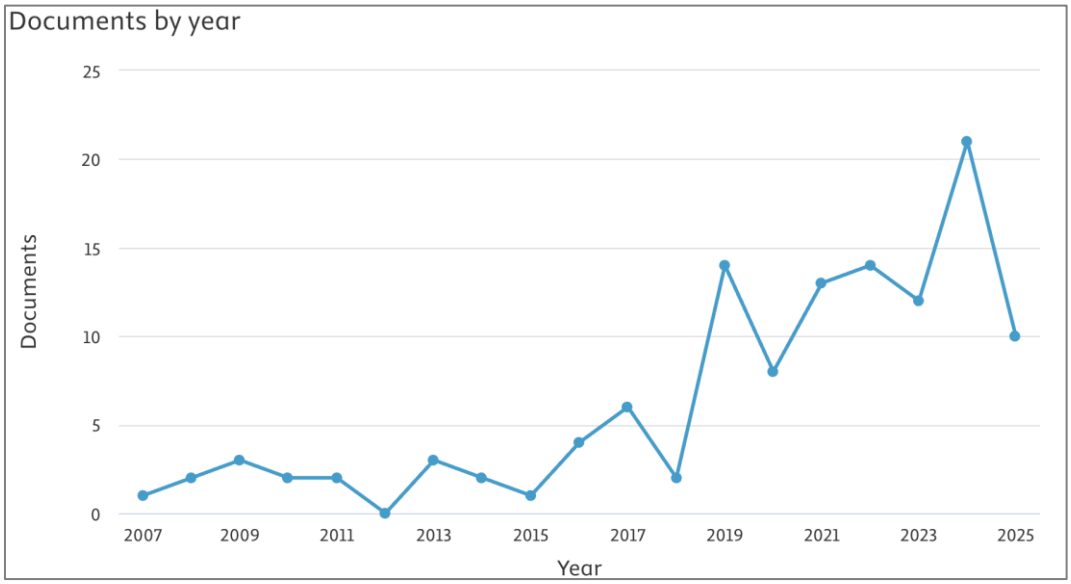


Figure 2. Number of Computer forensic focus on area digital forensics publications
Source: Scopus database

Since 2007, there has been little literature on computer forensics, particularly about digital forensics, due to a dearth of research published in credible journals, creating an opportunity for future scholars to bridge this gap. This research is critical for deepening understanding of the topic of computer forensics, particularly digital forensics, which influences both challenges and the development of computer forensics frameworks. This can help understand the practical and sustainable application of computer forensics, particularly around digital forensics, as well as the development of massive digitalization and the increasingly widespread use of AI, creating opportunities from the framework, trends in information or cyber security risk, supporting tools, and datasets.

RQ2: How are research investigations into computer forensics focused on the domain of digital forensics?

The analysis of the distribution research in the 120 articles was executed by categorizing the articles according to classifications such as nation, region, affiliation, source, and author, with a constraint of solely the top 10 articles in each classification. Acumen regarding the allocation of scholarship pertinent to computer forensics, particularly digital forensics will be advantageous for scholars and practitioners in elucidating the forthcoming research agenda, particularly in the sustainable advancement of the digital forensic paradigm.

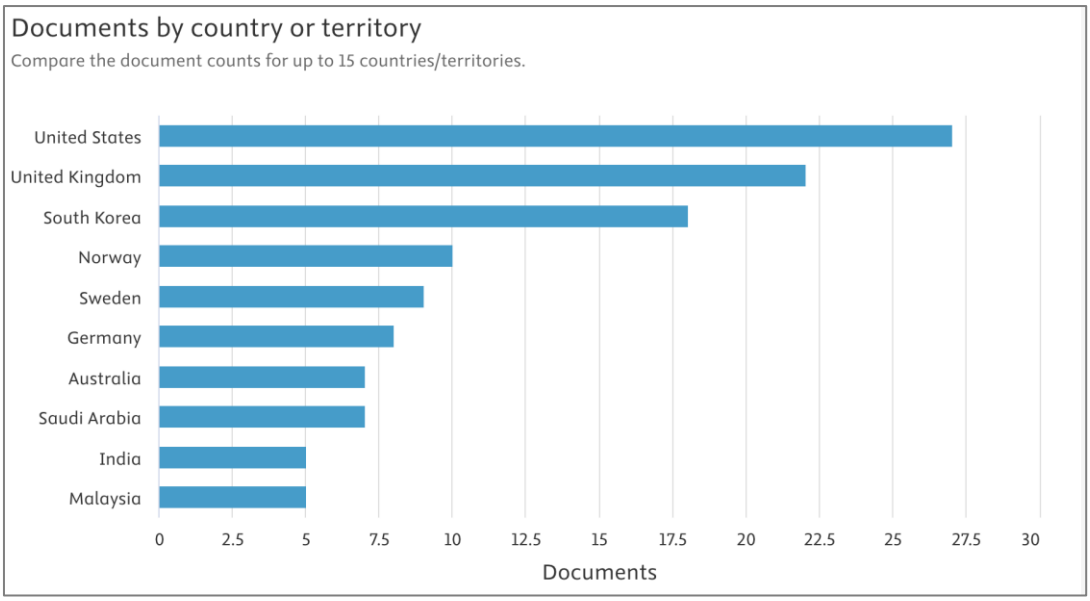


Figure 3. Top 10 Article by Country
Source: Scopus database

First, the distribution of research relevant to digital forensics classified by nation or geographical area is dominated by the United States with 27 articles, the United Kingdom with 22 articles, South Korea with 18 articles, Norway with 10 articles, Sweden with 9 articles, Germany with 8 articles, Australia, and Saudi Arabia with 7 articles, India, and Malaysia with 5 articles. (see Figure 3).

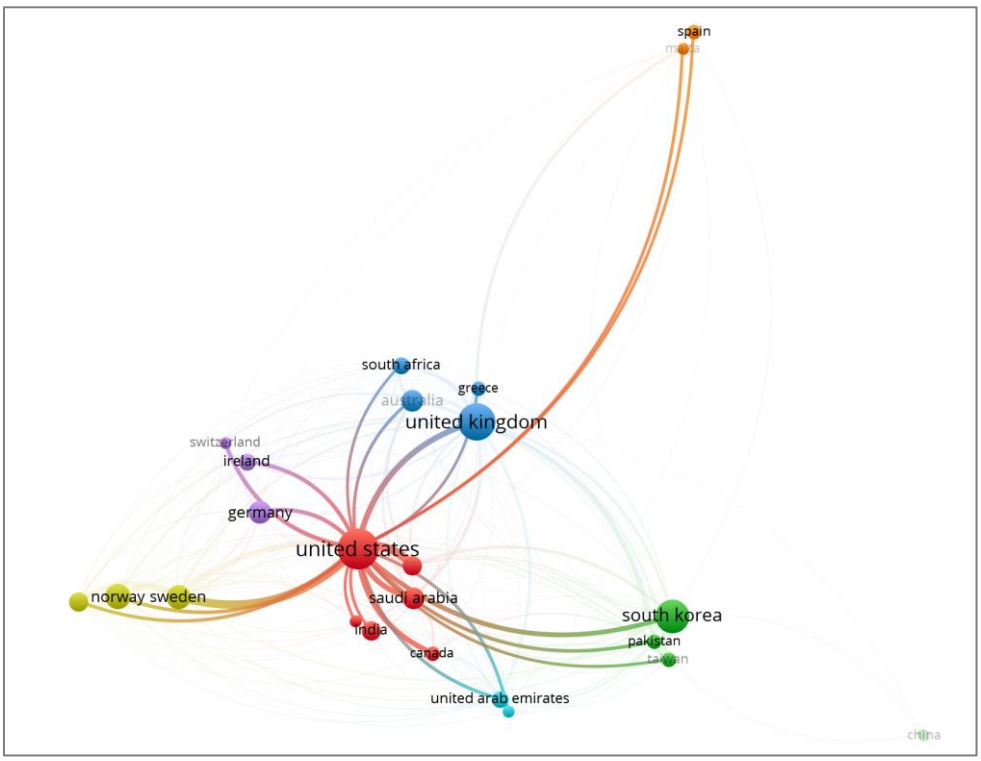


Figure 4. Network country visualization
Source: output VOS Viewer software

Second, these findings indicate that research in the field of computer forensics with specific digital forensics subjects is still dominated by developed countries such as United State and Europe, while countries in Asia and Africa are still relatively minimal (see Figure 4). This provides an opportunity for researchers from regions that still have minimal publications to contribute to this field, of course by finding research gaps to provide solutions to digital forensics activities that can be explored further such as methodological approaches using Artificial Intelligence, Machine Learning [17][28][29][30][31]. The allocation of scholarship pertinent to Computer forensic focus on area digital forensics predicated on institutional affiliations is predominantly

characterized by Korea University with 12 articles, Norges Teknisk-Naturvitenskapelige Universitet with 10 articles, Stockholms universitet and Norwegian Police University College with 5 articles, Rijksuniversiteit Groninge, University of New Haven, and LSU College of Engineering with 4 article. The findigs significant data, where Korean University was the only affiliate with the greatest productivity/number of affiliates in Asian countries (see Figure 5).

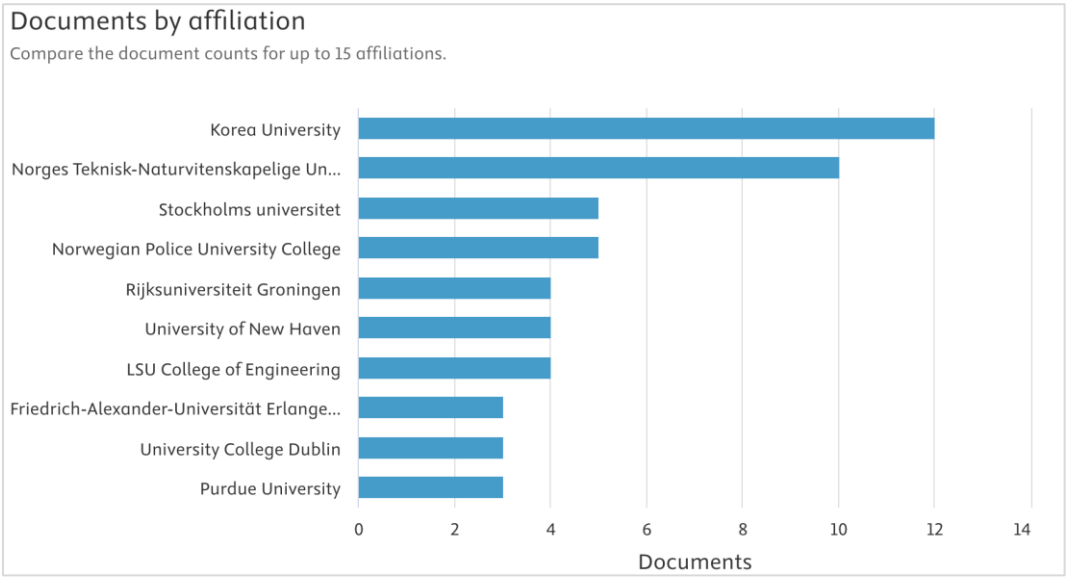
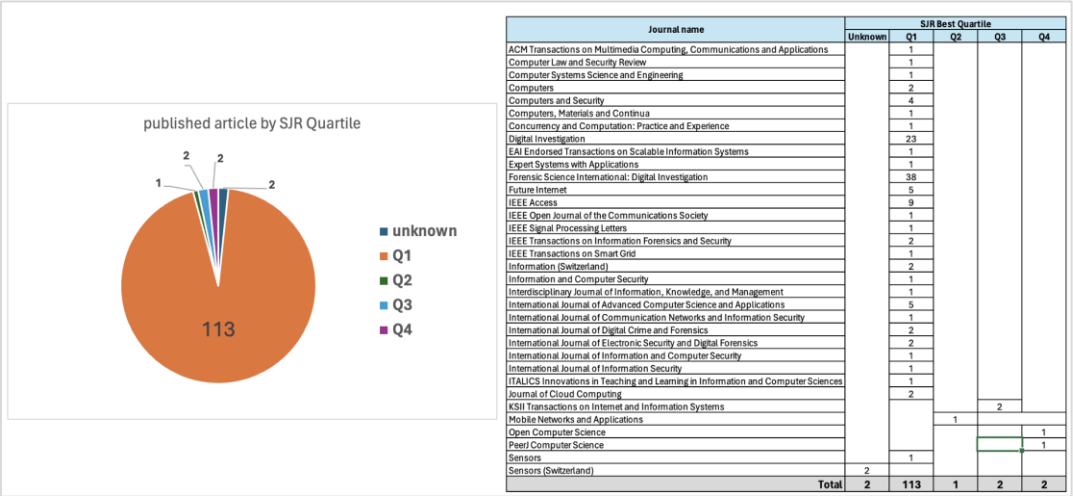


Figure 5. Top 10 of article by affiliation
Source: Scopus database



Journal name	SJR Best Quartile				
	Unknown	Q1	Q2	Q3	Q4
ACM Transactions on Multimedia Computing, Communications and Applications		1			
Computer Law and Security Review		1			
Computer Systems Science and Engineering		1			
Computers		2			
Computers and Security		4			
Computers, Materials and Continua		1			
Concurrency and Computation: Practice and Experience		1			
Digital Investigation		23			
EAI Endorsed Transactions on Scalable Information Systems		1			
Expert Systems with Applications		1			
Forensic Science International: Digital Investigation		38			
Future Internet		5			
IEEE Access		9			
IEEE Open Journal of the Communications Society		1			
IEEE Signal Processing Letters		1			
IEEE Transactions on Information Forensics and Security		2			
IEEE Transactions on Smart Grid		1			
Information (Switzerland)		2			
Information and Computer Security		1			
Interdisciplinary Journal of Information, Knowledge, and Management		1			
International Journal of Advanced Computer Science and Applications		5			
International Journal of Communication Networks and Information Security		1			
International Journal of Digital Crime and Forensics		2			
International Journal of Electronic Security and Digital Forensics		2			
International Journal of Information and Computer Security		1			
International Journal of Information Security		1			
ITALICS Innovations in Teaching and Learning in Information and Computer Sciences		1			
Journal of Cloud Computing		2			
KSII Transactions on Internet and Information Systems				2	
Mobile Networks and Applications			1		
Open Computer Science					1
PeerJ Computer Science					1
Sensors		1			
Sensors (Switzerland)	2				
Total	2	113	1	2	2

Figure 6. Number of Publishers based on SJR Quartile
Source: SJR Quartile, processed by the author

Third, according to the processed data, journals with quartile-1 (Q1) dominate the articles published by researchers, with a total of 113 articles, consisting of top 3 sources of journals, namely Forensic Science International: Digital Investigation (38), Digital Investigation (23), IEEE Access (9) and the remainder in other journals (see Figure 6).

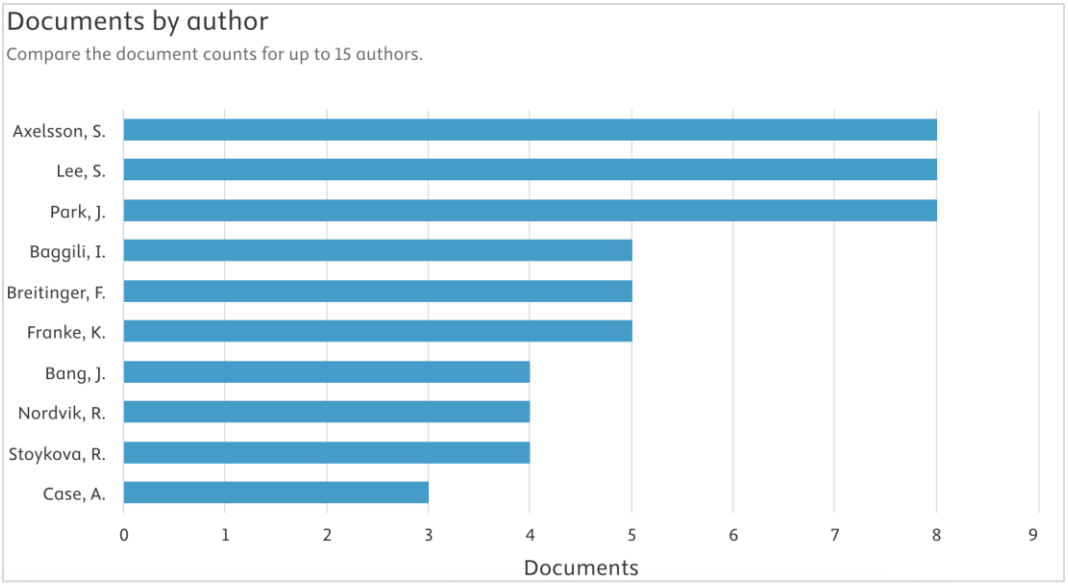


Figure 7. Count of publication by Top 10 authors
Source: Scopus database

Fourth, the distribution of research related to computer forensic focus on area digital forensics based on authors reveals no clear dominance. Among the top 10 authors, 3 of them (Axelsson, S.; Lee, S.; Park, J.) have each written 8 articles, 3 of them (Baggili, I.; Breitinger, F.; Franke, K.) have each written 5 articles, 3 of them (Bang, J.; Nordvik, R.; Stoykova, R.) have each written 4 articles, and (Case. A) has written 3 articles.

RQ3: What are the practical as well as theoretical implications for future research?

The examination included 120 manuscripts taken from the Scopus database. VOS viewer was used to demonstrate that the findings can have both theoretical and applied consequences for future computer forensics research, with a focus on digital forensics. The metadata analysis results obtained using VOS viewer will assist researchers and practitioners in better understanding the assumptions and conclusions connected to the subject area of digital forensics. The bibliometric analysis results obtained with VOS viewers can show which factors have been extensively investigated by previous researchers and which have not been researched sufficiently, setting the framework for future research. From a practitioner's perspective, the literature analysis results using VOS viewers will assist practitioners in applying computer forensics and focusing on digital forensics in the future. From Figure 8, the occurrences of digital forensics (120), computer forensics (116),electronic crime countermeasures (75), computer crime (41), forensic investigation (28), crime (21), digital evidence (20), digital storage (15), digital investigation (14), forensic engineering (13), metadata (12), digital device; file organization (11), memory; internet of things (10), malware (9), filesystem; forensic tools; cryptography; cloud forensics; incident response (8), machine learning; deep learning; convolutional neural network (2). Finally, these 10 most frequent keywords are shown in Table 2. The Total link strength section is obtained based on three minimum number of occurrences of a keyword, which explains the strength of keyword analysis and measures co-occurrence in one journal article document so that it can be used to identify the main topics regulated in this study, research trends, and relationships between concepts described based on significant keywords.

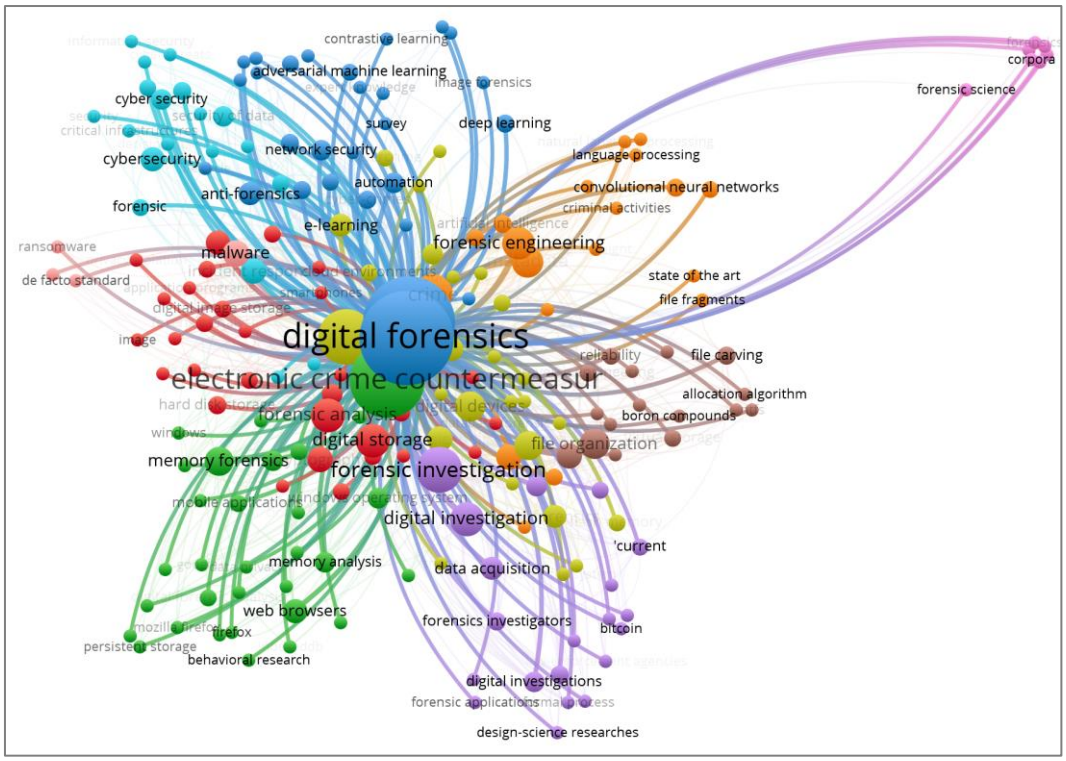


Figure 8. Co-occurance and Representation of Key Terms
Source: output VOSviewer software

Table 1. Keyword by authors

Rank	Keyword	Total Link Strength
1	digital forensics	712
2	computer forensics	701
3	electronic crime countermeasures	516
4	computer crime	315
5	forensic investigation	221
6	crime	179
7	digital evidence	146
8	digital storage	101
9	digital device	95
10	forensic engineering	95

Source: output VOSviewer software

Based on the findings of mapping and earlier research (see figure 3 and 5), shortcomings have been identified in previous studies, the majority of which were undertaken in affluent nations such as Europe and America. As a result, future research has a significant possibility to be undertaken in developing countries. According to data, ASEAN countries continue to perform less research in computer science and digital forensics. This study aims to fill gaps in previous research on computer forensics, particularly in digital forensics, by identifying more efficient mechanisms for decryption, data acquisition, and evidence analysis [32]. The findings from studies from computer forensic focus on digital forensic as a subject area by previous researcher show that attention should be paid to fundamental aspects that are key stage attribute conduct to digital forensic process. Below are the key stage attributes of digital forensics obtained from various references (see Figure 9). Figure 9 depicts the results of the analytical study in this study, demonstrating four essential stages in the deployment of digital forensics. These steps are derived from multiple prior studies and can be used as a foundation for carrying out digital forensic activities. They include the identification stage, the collecting stage, the analysis stage, and the maintenance stage. These steps serve as the foundation for this study, allowing us to examine each of its processes and discover information that is pertinent to the main topic, namely the application of AI in the digital forensics process. Figure 10 illustrates how AI has been used in prior studies to implement digital forensics.

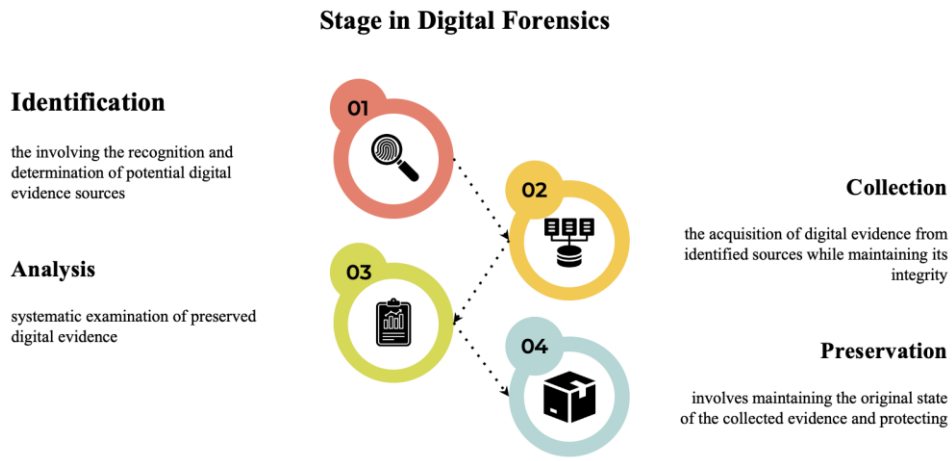


Figure 9. Digital Forensics stages
Source: adopted from previous research (Zareen et al., 2024; Adkins et al., 2024; Alqahtany & Syed, 2024; Felemban et al., 2024; (Ng et al., 2024; Chimmanee & Jantavongso, 2024; Ninos et al., 2025)

The digital forensics process consists of four critical phases:

1) Identification The identification stage entails finding and identifying potential sources of digital evidence, such as computers, servers, and computer-supporting equipment such as Internet of Things (IoT) sensors, network devices, and security devices [33].
2) Collection Once sources are identified, the collection phase entails gathering digital evidence while ensuring its integrity. Techniques such as bit-for-bit duplication are employed to preserve the original data, and specialized forensic tools are used to automate and validate this process [34][35]. However, the distributed nature of digital systems can complicate the evidence acquisition process [33].
3) Analysis Following collection, the analysis phase focuses on examining the acquired data to extract meaningful information and uncover digital patterns relevant to the investigation. This phase includes reviewing file metadata, timestamps, and user activities, often through advanced software suites [36][37]. With regard to developing data storage technologies, such as NoSQL databases, forensic analysis requires specialized frameworks to manage data complexity and heterogeneity [16].
4) Preservation The preservation phase ensures that digital evidence remains intact, authentic, and legally admissible from the time of acquisition through to its potential use in court. This phase relies on standardized models like the Open Archival Information System (OAIS) and PREMIS to secure the long-term reliability of stored evidence [38][39][40].

The effective application of these phases ensures forensic soundness, procedural rigor, and the evidential value of digital artifacts in legal and investigative contexts. Thus, each stage of digital forensics must be carried out with accuracy, adhering to best practices to ensure that digital evidence stays valid, reliable, and legally acceptable.

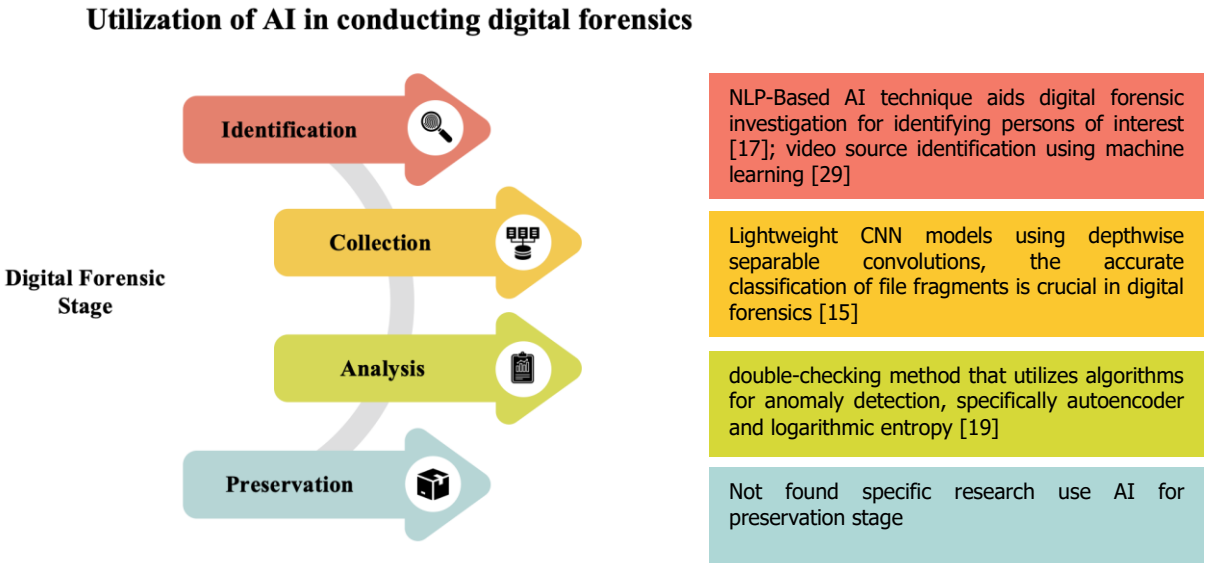


Figure 10. utilization of AI in cond*uction digital forensic by previous researcher*
Source: adopted from previous research

According to the findings of the investigation, various researchers apply artificial intelligence at each stage of digital forensics to attain the intended outcomes. Figure 10 shows how researchers utilize AI to address challenges and achieve their aims.

4.2 Discussion

The development of artificial intelligence (AI) technology has brought significant transformation to the field of digital forensics, with various research studies demonstrating that AI implementation can enhance efficiency and accuracy in every stage of the digital forensic process. Lightweight CNN models have been developed using depth-wise separable convolutional neural networks to improve analysis efficiency while reducing computational complexity, achieving 79% accuracy on the FFT-75 dataset with nearly 100,000 parameters and delivering a fourfold reduction in model size with sixfold increase in processing speed, making them highly suitable for resource-constrained forensic environments [15]. Natural Language Processing (NLP) technology has emerged as a valuable tool for digital forensic investigations, particularly in emotion categorization to identify persons of interest by detecting higher displays of negative emotions that are frequently indicative of exposure to or involvement in criminal activities [17]. Autoencoder-based analysis addresses the time-consuming and labor-intensive nature of manual suspicious trace identification by incorporating a pre-processing stage where artifacts are filtered based on user-defined features, employing autoencoder-based prioritization techniques with loss value calculations to assess relevance and anomaly levels, applying logarithmic entropy algorithms to distinguish between typical and suspicious data patterns, and integrating double-checking mechanisms for anomaly detection to improve accuracy and reliability [19]. Furthermore, video source identification has become crucial for addressing cybercrimes involving video content, where a machine learning-based methodology utilizing features extracted from video metadata and storage formats, enhanced with SMOTE and K-Fold cross-validation techniques, has achieved excellent identification accuracy of approximately 99.96% across 1,974 sample videos from 16 different instant messaging services, effectively addressing the challenge of lost or altered metadata when videos are shared through instant messaging applications [29]. These AI approaches collectively demonstrate the transformative potential of artificial intelligence in enhancing digital forensic capabilities across multiple domains and investigation scenarios.

5. Conclusion

The study investigates 120 academic publications from the Scopus collection and presents numerous key findings. Investigations into digital forensics have been extremely scarce, as seen by the first paper published in 2007. Research on digital forensics is being disseminated in numerous countries, though the distribution is variable. Digital forensics investigations continue to be primarily conducted in industrialized countries such as the United States and Europe, with contributions from Asia and Africa remaining insufficient. This may be due to a combination of insufficient training, inadequate legal infrastructure, and technological and socioeconomic constraints. These factors contribute to a growing gap in the use of AI in digital forensics, necessitating comprehensive capacity-building activities and strategic investments to increase investigative capacities in the digital era, including collaborative research efforts. The digital forensics process is divided into four phases: identification, collection, analysis, and preservation. The research has examined the use of artificial intelligence (AI) in digital forensics. In the identification stage, researchers use NLP-Based AI and several machine learning methods for video source identification as digital evidence. In the collection stage, they use lightweight CNN models using depthwise separable convolutions; the accurate classification of file fragments is crucial in digital forensics. In the analysis stage, researchers use autoencoder and logarithmic entropy for anomaly detection. However, no use of AI for the preservation stage was found.

Artificial intelligence (AI) has reshaped the field of digital forensics by increasing the accuracy, efficiency, and overall efficacy of investigation procedures. However, the integration of AI technologies raises several ethical concerns, including algorithmic bias, concerns about data privacy, and a lack of transparency in decision-making processes. To ensure the responsible and equitable use of AI in digital forensics, it is essential to address these concerns by implementing explainable AI models, developing standardized protocols, and promoting interdisciplinary collaboration among technologists, legal experts, and ethicists. The researchers acknowledge that the study had certain limitations; the analysis is based entirely on papers taken from the Scopus database, which may limit generalizability. Future studies are expected to combine findings from both the Scopus and Web of Science databases to improve the research's comprehensiveness and quality. Subsequent inquiries may also delve into specialized domains within this field, including the use of artificial intelligence in evidence discovery and inference throughout the digital forensic phases, especially in the preservation phase.

Furthermore, the use of Artificial Intelligence (AI) in digital forensics has substantially increased the effectiveness of investigations, but it also brings a few technological challenges. In terms of effectiveness, AI accelerates and improves the accuracy of large-scale data analysis using technologies such as machine learning and natural language processing. Artificial intelligence can automate investigation methods, simplify evidence interpretation, and reduce manual workload. However, the black box nature of many AI models causes technological issues in terms of transparency and trust, necessitating the development of Explainable AI to ensure that AI decision-making processes are understood and legally acceptable. While a rigorous methodology was used to reduce interpretational bias, future studies may use new research techniques to supplement the findings of this analysis.

References

[1] Nelufule, N., Singano, T., & Masango, M. (2024). A comprehensive exploration of digital forensics investigations in embedded systems, ubiquitous computing, fog computing, and edge computing. In *7th International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems, icABCD 2024 - Proceedings*. IEEE. https://doi.org/10.1109/icABCD62167.2024.10645254

[2] Fakhouri, H. N., Alsharaiah, M. A., Al Hwaitat, A. K., Alkalaileh, M., & Dweikat, F. F. (2024). Overview of challenges faced by digital forensic. In *2nd International Conference on Cyber Resilience, ICCR 2024*. IEEE. https://doi.org/10.1109/ICCR61006.2024.10532850

[3] Firdonsyah, A., Purwanto, P., & Riadi, I. (2023). Framework for digital forensic ethical violations: A systematic literature review. In *E3S Web of Conferences* (Vol. 448, Article 01003). EDP Sciences. https://doi.org/10.1051/e3sconf/202344801003

[4] Adel, A., Ahsan, A., & Davison, C. (2024). ETHICore: Ethical compliance and oversight framework for digital forensic readiness. *Information*, *15*(6), Article 363. https://doi.org/10.3390/info15060363

[5] Mpungu, C., George, C., & Mapp, G. (2023). Developing a novel digital forensics readiness framework for wireless medical networks using specialised logging. In *Advanced Sciences and Technologies for Security Applications* (pp. 203-226). Springer. https://doi.org/10.1007/978-3-031-20160-8_12

[6] Akotoye, F. X. K., Adeyemi, R. I., & Venter, H. S. (2020). A study on problems of behaviour-based user attribution in computer forensic investigation. In *European Conference on Information Warfare and Security, ECCWS* (pp. 458-465). https://doi.org/10.34190/EWS.20.117

[7] Rawat, R., Oki, O. A., Chakrawarti, R. K., Adekunle, T. S., Lukose, J. M., & Ajagbe, S. A. (2023). Autonomous artificial intelligence systems for fraud detection and forensics in dark web environments. *Informatica*, *47*(9), 51-62. https://doi.org/10.31449/INF.V46I9.4538

[8] Dimpe, P. M., & Kogeda, O. P. (2018). Generic digital forensic requirements. In *2018 Open Innovations Conference, OI 2018* (pp. 240-245). IEEE. https://doi.org/10.1109/OI.2018.8535924

[9] Chin, J. M., Arabia, A.-M., McKinnon, M., Page, M. J., & Searston, R. A. (2024). A plan for systematic reviews for high-need areas in forensic science. *Forensic Science International: Synergy*, *9*, Article 100542. https://doi.org/10.1016/j.fsisyn.2024.100542

[10] Alharbi, S., Weber-Jahnke, J., & Traore, I. (2011). The proactive and reactive digital forensics investigation process: A systematic literature review. *International Journal of Security and its Applications*, *5*(4), 59-72.

[11] Nelufule, N., Singano, T., & Masango, M. (2024). A comprehensive exploration of digital forensics investigations in embedded systems, ubiquitous computing, fog computing, and edge computing. In *7th International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems, icABCD 2024 - Proceedings*. IEEE. https://doi.org/10.1109/icABCD62167.2024.10645254

[12] Firdonsyah, A., Purwanto, P., & Riadi, I. (2023). Framework for digital forensic ethical violations: A systematic literature review. In *E3S Web of Conferences* (Vol. 448, Article 01003). EDP Sciences. https://doi.org/10.1051/e3sconf/202344801003

[13] Zareen, M. S., Aslam, B., Tahir, S., Rasheed, I., & Khan, F. (2024). Unveiling the dynamic landscape of digital forensics: The endless pursuit. *Computers*, *13*(12), Article 333. https://doi.org/10.3390/computers13120333

[14] Alqahtany, S. S., & Syed, T. A. (2024). ForensicTransMonitor: A comprehensive blockchain approach to reinvent digital forensics and evidence management. *Information*, *15*(2), Article 109. https://doi.org/10.3390/info15020109

[15] Felemban, M., Ghaleb, M., Saaim, K., Alsaleh, S., & Almulhem, A. (2024). File fragment type classification using light-weight convolutional neural networks. *IEEE Access*, *12*, 157179-157191. https://doi.org/10.1109/ACCESS.2024.3486180

[16] Singh, A., Singh, S. K., Vege, H. K., & Singh, N. (2022). A framework for crime detection and diminution in digital forensics (CD3F). *International Journal of Advanced Computer Science and Applications*, *13*(9), 332-345. https://doi.org/10.14569/IJACSA.2022.0130939

[17] Adkins, J., Al Bataineh, A., & Khalaf, M. (2024). Identifying persons of interest in digital forensics using NLP-based AI. *Future Internet*, *16*(11), Article 426. https://doi.org/10.3390/fi16110426

[18] Ninos, F., Karalas, K., Dechouniotis, D., & Polemis, M. (2025). On microservice-based architecture for digital forensics applications: A competition policy perspective. *Future Internet*, *17*(4), Article 137. https://doi.org/10.3390/fi17040137

[19] Kim, J., Son, B., Yu, J., & Yun, J. (2024). AI-driven prioritization and filtering of Windows artifacts for enhanced digital forensics. *Computers, Materials & Continua*, *81*(2), 3371-3393. https://doi.org/10.32604/cmc.2024.057234

[20] Purnaye, P., & Kulkarni, V. (2022). BiSHM: Evidence detection and preservation model for cloud forensics. *Open Computer Science*, *12*(1), 154-170. https://doi.org/10.1515/comp-2022-0241

[21] Todd, M. C., & Peterson, G. L. (2024). Temporal metadata analysis: A learning classifier system approach. *Forensic Science International: Digital Investigation*, *51*, Article 301842. https://doi.org/10.1016/j.fsidi.2024.301842

[22] Maia, E., Sousa, N., Oliveira, N., Wannous, S., Sousa, O., & Praça, I. (2022). SMS-I: Intelligent security for cyber–physical systems. *Information*, *13*(9), Article 403. https://doi.org/10.3390/info13090403

[23] Oh, D. B., Kim, D., & Kim, H. K. (2024). volGPT: Evaluation on triaging ransomware process in memory forensics with Large Language Model. *Forensic Science International: Digital Investigation*, *49*, Article 301756. https://doi.org/10.1016/j.fsidi.2024.301756

[24] Chimmanee, K., & Jantavongso, S. (2024). Digital forensic of Maze ransomware: A case of electricity distributor enterprise in ASEAN. *Expert Systems with Applications*, *249*, Article 123652. https://doi.org/10.1016/j.eswa.2024.123652

[25] Ng, M., James, J., & Bull, R. (2024). 'What you say in the lab, stays in the lab': A reflexive thematic analysis of current challenges and future directions of digital forensic investigations in the UK. *Forensic Science International: Digital Investigation*, *51*, Article 301839. https://doi.org/10.1016/j.fsidi.2024.301839

[26] Chanthiran, M., Ibrahim, A., Abdul Rahman, M. H., Kumar, S., & Dandage, D.-R. (2022, June). A systematic literature review with bibliometric meta-analysis of AI technology adoption in education. *EDUCATUM Journal of Science, Mathematics and Technology*, *9*, 61-71. https://doi.org/10.37134/ejsmt.vol9.sp.7.2022

[27] Buchholz, F., & Spafford, E. H. (2007). Run-time label propagation for forensic audit data. *Computers & Security*, *26*(7-8), 496-513. https://doi.org/10.1016/j.cose.2007.07.002

[28] Khalid, Z., Iqbal, F., & Fung, B. C. M. (2024). Towards a unified XAI-based framework for digital forensic investigations. *Forensic Science International: Digital Investigation*, *50*, Article 301806. https://doi.org/10.1016/j.fsidi.2024.301806

[29] Yang, H., Kim, J., & Park, J. (2024). Video source identification using machine learning: A case study of 16 instant messaging applications. *Forensic Science International: Digital Investigation*, *50*, Article 301812. https://doi.org/10.1016/j.fsidi.2024.301812

[30] Kao, H.-H. (2025). Accelerating multilingual cryptocurrency forensics: An NLP-driven approach for efficient mnemonic identification. *IEEE Access*, *13*, 10513-10526. https://doi.org/10.1109/ACCESS.2025.3528829

[31] Joseph, D. P., & Perumal, V. (2025). Optimizing forensic file classification: Enhancing SFCS with βk hyperparameter tuning. *PeerJ Computer Science*, *11*, Article e2608. https://doi.org/10.7717/peerj-cs.2608

[32] Nisioti, A., Loukas, G., Laszka, A., & Panaousis, E. (2021). Data-driven decision support for optimizing cyber forensic investigations. *IEEE Transactions on Information Forensics and Security*, *16*, 2397-2412. https://doi.org/10.1109/TIFS.2021.3054966

[33] Obioha, J. I., Mohan, A. P., & Louafi, H. (2023). Digital evidence collection in IoT environment. In *Innovations in Digital Forensics* (pp. 263-292). World Scientific. https://doi.org/10.1142/9789811273209_0008

[34] Steele, J. (2007). Digital forensics and analyzing data. In *Alternate Data Storage Forensics* (pp. 1-38). Syngress. https://doi.org/10.1016/B978-159749163-1/50001-9

[35] Barrère, M., Betarte, G., & Rodriguez, M. (2011). Towards machine-assisted formal procedures for the collection of digital evidence. In *2011 9th Annual International Conference on Privacy, Security and Trust, PST 2011* (pp. 32-35). IEEE. https://doi.org/10.1109/PST.2011.5971960

[36] Bryant, R. (2016). Criminological and psychological perspectives. In *Policing Digital Crime* (pp. 43-61). Routledge. https://doi.org/10.4324/9781315601083-8

[37] Kennedy, I., & Day, E. (2016). Digital forensic analysis. In *Policing Digital Crime* (pp. 161-185). Routledge. https://doi.org/10.4324/9781315601083-14

[38] Abdul-Samad, A., Md Siraj, M., Hajar Othman, S., Hafiz Rahman, M., & Zaharudin Ahmad Darus, M. (2024). Comprehensive review on data preservation models and standards in digital forensic. In *2024 International Conference on Data Science and Its Applications, ICoDSA 2024* (pp. 277-282). IEEE. https://doi.org/10.1109/ICoDSA62899.2024.10651616

[39] Granja, F. M., & Rafael, G. D. R. (2015). Preservation of digital evidence: Application in criminal investigation. In *Proceedings of the 2015 Science and Information Conference, SAI 2015* (pp. 1284-1292). IEEE. https://doi.org/10.1109/SAI.2015.7237309

[40] Granja, F. M., & Rodríguez, G. (2015). Digital preservation and criminal investigation: A pending subject. In *Advances in Intelligent Systems and Computing* (pp. 299-309). Springer. https://doi.org/10.1007/978-3-319-16486-1_30.