# Evolution and Research Opportunities of Digital Forensic Tools: A Bibliometric Analysis

**Rischi Dwi Syahputri*[1], Alexander Anggono[2], Prasetyono[3], Mohamad Djasuli[4]**
[1,2,3,4]Universitas Trunojoyo Madura; Jl. Raya Telang PO BOX 2 Kamal, Bangkalan
[1]Magister Akuntansi, Fakultas Ekonomi dan Bisnis, Universitas Trunojoyo Madura
e-mail: ***[1]230251100008@student.trunojoyo.ac.id**, [2]alexander.anggono@trunojoyo.ac.id
[3]prasetyono_akt@trunojoyo.ac.id , [4]djasuli@trunojoyo.ac.id

***Abstract***

*The rapid growth of digital technology has introduced challenges like cybercrime, online fraud, and money laundering. Digital forensic tools play a critical role in investigating and analyzing electronic evidence to address these threats. Therefore, research and development in the field of digital forensics is crucial to address the growing digital security challenges. This study aims to conduct a bibliometric analysis of digital forensic tools research in the business, management, and accounting domains over the past decade, evaluate the evolution of the research, identify promising research opportunities, and provide insights into future directions in the field. Using VOSviewer software, 698 Scopus-indexed articles from ScienceDirect during 2014–2023 were analyzed. The analysis revealed key insights, such as the central collaborative roles of researchers like Frank Breitinger and Ibrahim Baggili, who have made significant contributions to advancing the field. Despite the progress, the analysis identifies research gaps in areas like mobile forensics, cloud forensics, malware analysis, and anti-forensics, underscoring opportunities for innovation. Key recommendations include expanding research to other databases, addressing gaps in ethical and privacy concerns in digital investigations, and leveraging emerging technologies like explainable AI and blockchain to enhance the reliability and effectiveness of digital forensic tools.*

***Keywords***— Cybersecurity, Digital Forensic Tools, Research Trends, Bibliometric Analysis

## 1. INTRODUCTION

Over the past decade, there has been a significant increase in the use of digital technology, leading to new challenges related to digital threats such as cybercrime, online fraud, and money laundering [1]. To address these threats, digital forensic tools have become crucial in investigating and analyzing electronic evidence to combat increasingly complex and widespread digital crimes. These tools are not only used to uncover digital crimes but also to trace digital footprints and ensure information security, leading to a significant increase in research and development in digital forensic technology [2].

In the realm of digital forensics, institutions, and law enforcement departments utilize various digital forensic tools, both commercial and open-source, to examine digital evidence [2]. Research has shown that these digital forensic tools play a vital role in addressing evolving digital security challenges, encompassing areas such as computer forensics, network forensics, mobile forensics, cloud forensics, and IoT forensics [3]. Additionally, research focuses on developing techniques and tools for digital forensics investigations in cybercrimes, including forensic analysis of social media applications and instant messaging platforms like MiChat and Signal Messenger. In this context, the DFRWS (Digital Forensic Research Workshop) framework has been used to identify, preserve, collect, examine, analyze, and present digital evidence [4][5][6].

As digital forensic advancements progress, researchers have proposed a proactive approach to digital forensic readiness in cloud computing environments, emphasizing risk management, incident handling principles, and legal compliance [7][8][9]. Forensic accounting techniques, such as data mining, password protection, sampling discovery, ratio analysis, and Benford's Law, are recognized as valuable tools for fraud detection [10].

Furthermore, research highlights the importance of digital forensics in combating increasingly complex financial crimes and money laundering threats, focusing on developing techniques and tools to counter these threats [11]. Moreover, the testing of digital forensic tools is crucial, especially in addressing anti-forensic challenges, representing a significant step forward in testing digital forensic tools [12].

The significance of developing digital forensic tools is evident in research that integrates digital forensics into existing digital workflows, such as the BitCurator project. This project aims to enhance documentation, interfaces, and functionality in processing digital archive materials [13]. However, it is noted that the development of digital forensic tools is often conducted independently rather than collaboratively [14]. Testing these tools necessitates appropriate testing techniques and relevant testing data for various categories of digital forensic tools [15].

Regarding fraud detection, a performance analysis of digital forensic tools on the Android platform and the MiChat application has been carried out using the ACPO and DFRWS frameworks [4]. The analysis results suggest that the most valuable digital evidence comprises chat texts and contacts, which can be utilized to substantiate legal claims. Bibliometric analysis of digital forensics for fraud detection indicates a growing interest in this research area. The utilization of digital forensic tools for fraud detection has attracted attention due to their potential to effectively identify fraudulent activities. Various studies have emphasized the importance of digital forensic tools in fraud detection, highlighting their effectiveness in uncovering fraudulent activities [16][17]. Moreover, the integration of digital analysis models in the fight against economic crime has been suggested to bridge the gap between physical and digital investigations, thereby increasing the effectiveness of the fraud detection process [18].

In addition, the application of computer forensic tools, such as Autopsy, BHE, and Net Analysis, in web browser forensic analysis has been highlighted as an important aspect of digital forensic investigations to uncover criminal activity in web browsers [19]. The role of digital forensic experts in cybercrime investigations has been emphasized, highlighting the need for technical skills in operating digital forensic tools for effective crime analysis [20].

Hence, research and development in the field of digital forensics are vital in addressing evolving digital security challenges. With the increasing prevalence of cybercrime, there is a crucial need to enhance the speed and performance of digital forensic tools to keep pace with criminal activities [21]. Ensuring the dependence and reliability of digital forensic tools through data recovery function testing is crucial, especially considering that the data processed by these tools serve as evidence in legal proceedings [22].

Bibliometric analysis, as a method to measure and analyze scientific literature, provides deep insights into the evolution and direction of research in this field. Through bibliometric analysis, key trends, notable scholarly contributions, and under-explored research opportunities can be identified. To perform the bibliometric analysis, this study utilizes VOSviewer, a specialized software designed for creating and visualizing bibliometric networks such as co-authorship, co-occurrence, and citation patterns. VOSviewer has been widely used in bibliometric studies across various fields. For instance, Karyana et al. used VOSviewer to analyze 344 articles on computational thinking in science education, revealing a peak in research activity in 2020 [23]. Similarly, Genç and Koçak utilized the tool to examine 867 studies on artificial intelligence in science education, mapping trends and identifying prolific authors [24]. In another example, Guofang et al. analyzed 592 articles on university-industry collaboration, identifying influential institutions and thematic trends, showcasing VOSviewer's versatility in handling diverse academic contexts [25]. By leveraging VOSviewer, this study maps the progress and identifies gaps in digital forensics research, providing a clearer picture of innovation and collaboration trends in the field. This is critical to understanding how digital forensics technology has evolved over the past decade and where it is headed in the future. The scope of this research is that the author only uses data from Scopus-indexed articles published in the last 10 (ten) years, and the articles are available through the ScienceDirect website. The selection of the ScienceDirect database is based on the fact that to date, ScienceDirect is one of the leading and largest scientific literature provider platforms in the field of science.

This study aims to conduct a bibliometric analysis of digital forensic tools research over the past ten years, evaluate the evolution of the technology, identify promising research opportunities, and provide insights into future directions in the field. In doing so, it is expected to make a valuable contribution to researchers, practitioners, and policymakers in their efforts to develop and implement more effective and efficient digital forensic technologies.

## 2. RESEARCH METHODS

This study will use a bibliometric approach to analyze trends in digital forensic tools research publications, as well as identify future research opportunities. The bibliometric approach allows researchers to systematically explore and analyze relevant literature in the domain under study. Data for this bibliometric analysis will be collected through the Scopus database downloaded from the ScienceDirect website, which is a trusted and comprehensive source of information in the field of science. The data collection process will follow the steps suggested by Moher et al., referred to as the PRISMA method, which includes identification, screening, eligibility assessment, and inclusion [26].

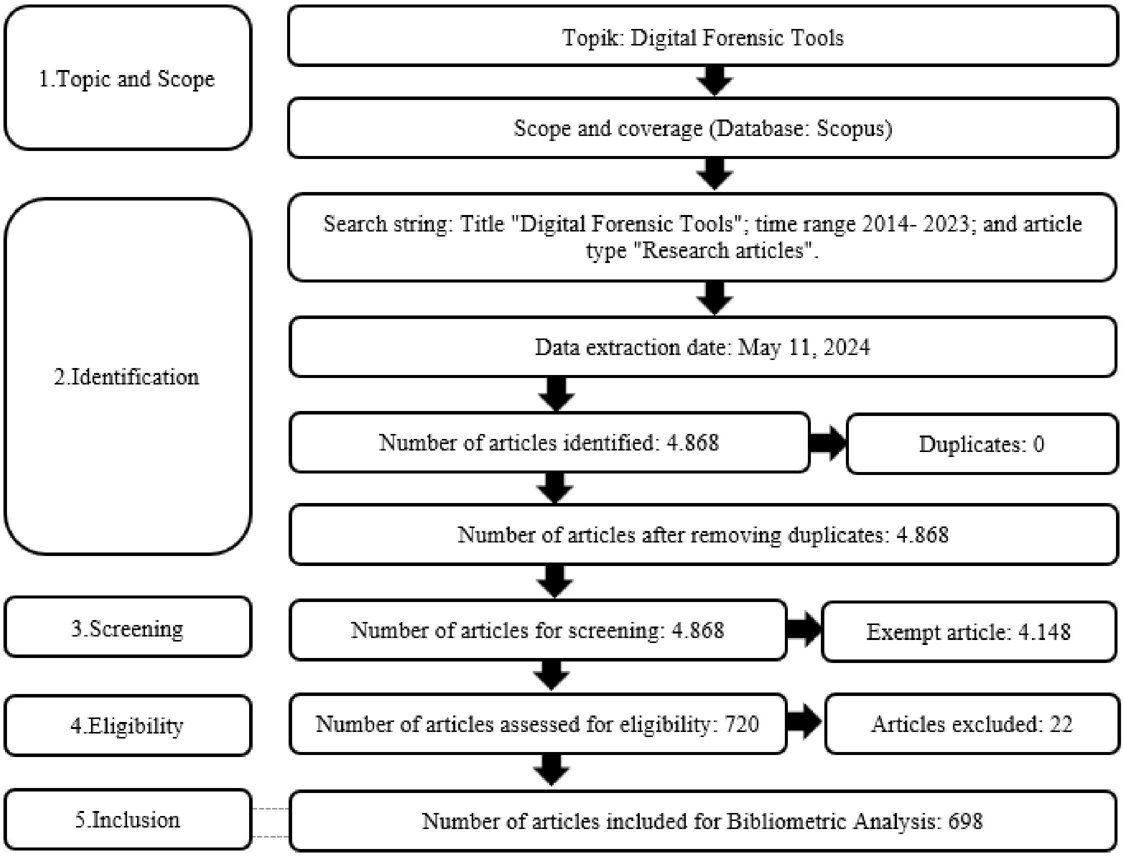
1.Topic and Scope
Topik: Digital Forensic Tools
Scope and coverage (Database: Scopus)
2.Identification
Search string: Title "Digital Forensic Tools"; time range 2014- 2023; and article type "Research articles".
Data extraction date: May 11, 2024
Number of articles identified: 4.868
Duplicates: 0
Number of articles after removing duplicates: 4.868
3.Screening
Number of articles for screening: 4.868
Exempt article: 4.148
4.Eligibility
Number of articles assessed for eligibility: 720
Articles excluded: 22
5.Inclusion
Number of articles included for Bibliometric Analysis: 698

Figure 1. Data collection process using the PRISMA Method

The identification process will involve searching and collecting relevant scientific publications using search terms that match the scope of the study. Thereafter, publications will be screened according to predefined inclusion and exclusion criteria to ensure that only relevant and high-quality publications will be included in the bibliometric analysis. An eligibility assessment will be conducted to evaluate the suitability of each publication to the research objectives, while the inclusion step will ensure that only publications that meet the set criteria will be included in the analysis. Using this approach, it is hoped that this study can provide in-depth knowledge about current research trends in digital forensic tools, as well as identify research opportunities that can guide future research directions in this important domain. The data collection steps are shown in Figure 1.

The first step is to identify research by entering the keyword "Digital Forensic Tools", the publication time span of the last 10 years from 2014 to 2023, and only selecting the type of article "Research articles" in the Scopus database. Data retrieval was carried out on May 11, 2024. At this stage, 4,868 articles were obtained according to the first step criteria. Of these 4,868 articles, no duplicate articles were found, so they can proceed to the next stage. Furthermore, the second stage is a screening process where only articles with the subject area "Business, Management and Accounting" are included for the next process. As a result, 720 articles were selected after screening 4,148 articles at this stage. In the third stage, the authors assessed the eligibility of the articles where 22 articles that did not provide abstracts and keywords were excluded from the study. In the final stage, the authors included the remaining 698 articles and saved them in (.RIS) format for review using the help of VOSviewer software. This is because bibliometric analysis procedures often involve the use of specialized software such as VOSviewer to visualize bibliometric data and identify relationships between various elements in the literature under study. [27][28]. In addition, a graph displaying the number of articles published each year was processed with Ms. Excel 2021.

## 3. RESULT AND DISCUSSION

### *3.1. Publication Trends*

The publication trends related to digital forensic tools research in the last ten years are shown in Figure 2. From the figure, it can be seen that over the last decade, there have been fluctuations in the number of publications related to digital forensic tools with a total publication of 698 articles. The graph shows the trend of article publication from 2014 to 2023. In 2014, the number of articles published was 54 articles. This figure decreased in 2015 to 47 articles. Then, there was a slight increase in 2016 with 53 articles. In 2017, the number of publications increased significantly to 60 articles. However, in 2018, the number of articles decreased slightly to 58 articles. In 2019, the number of publications increased again to 68 articles and this number remained the same in 2020. The year 2021 saw a considerable spike in the number of articles published, with a total of 106 articles. After that, in 2022, the number of publications decreased to 85 articles. In 2023, the number of published articles rose again to 99 articles.

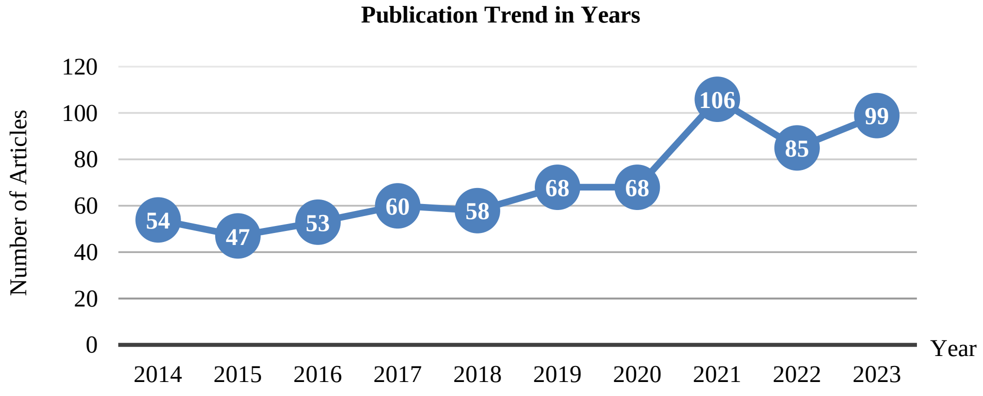

*Figure 2: Publication Trends in Years*

The graph shows the trend of article publication from 2014 to 2023. In 2014, the number of articles published was 54 articles. This figure decreased in 2015 to 47 articles. Then, there was a slight increase in 2016 with 53 articles. In 2017, the number of publications increased significantly to 60 articles. However, in 2018, the number of articles decreased slightly to 58 articles. In 2019, the number of publications increased again to 68 articles and this number remained the same in 2020. The year 2021 saw a considerable spike in the number of articles published, with a total of 106 articles. After that, in 2022, the number of publications decreased to 85 articles. In 2023, the number of published articles rose again to 99 articles.

Overall, there is an increasing trend in the number of article publications with fluctuations every year, and the peak occurred in 2021. This trend shows a significant increase in the number of publications, reflecting the growing interest and growing contribution of the use of digital forensic tools in the scope of accounting, management, and business sciences.

### 3.2. Author Network Analysis

The author collaboration network visualization using VOSviewer in Figure 3 displays the collaborative relationships between authors over the period 2014 to 2023. In this diagram, each node represents an author, while the connecting lines indicate the level of collaboration between them. This author relationship map generated by VOSviewer shows the collaboration network among researchers in the field of digital forensics from 2014 to 2023. The interconnected dots indicate authors who have collaborated on research, while the size and color intensity of the dots illustrate the frequency and timing of collaboration.

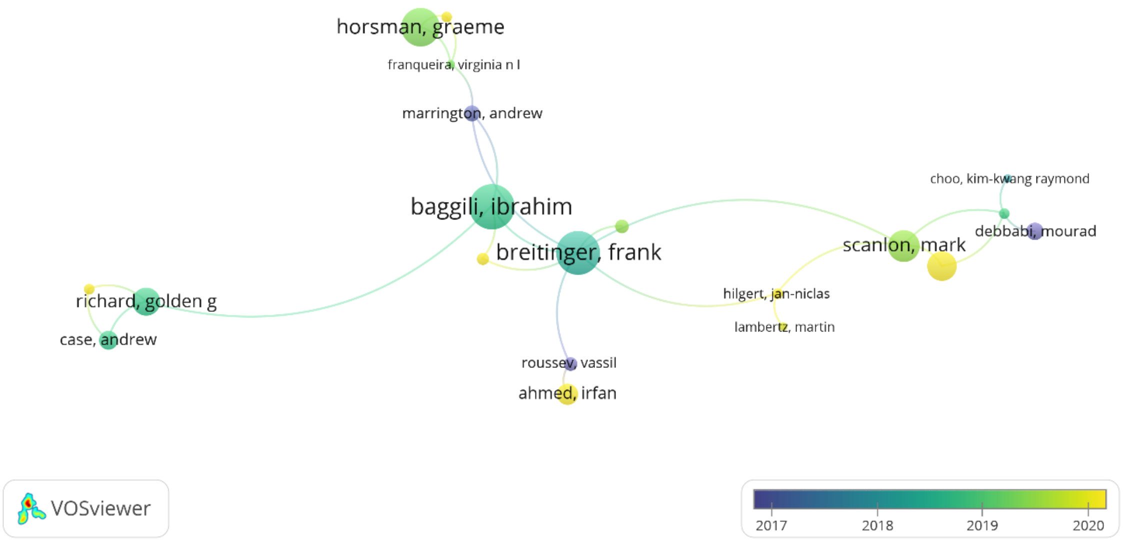

*Figure 3: Co-Authorship Results (Overlay Visualization)*

In the center of the map, Frank Breitinger and Ibrahim Baggili emerge as central figures with many connections, showing that they often collaborated with various other researchers, such as Graeme Horsman, Virginia I. Franqueira, and Andrew Marrington. This shows their central role in the digital forensics research community. On the right side of the map, Mark Scanlon and Nhien-An Le-Khac are also seen as important points, with many connections linking them to other researchers such as Elias Bou-Harb, Mourad Debbabi, and Kim-Kwang Raymond Choo. These connections show that they are also key collaborators in this field. On the left side, there is a smaller cluster of researchers, with Richard Golden G and Andrew Case as the main figures, showing more limited but still significant collaborations in certain contexts. Overall, this map illustrates the dynamics of research collaboration in digital forensics, showing several central figures who have been instrumental in shaping collaboration networks and driving research in this area. This indicates that digital forensic tools research is evolving through extensive collaboration among various researchers and institutions.

### 3.3. Keyword Network Analysis

Figure 4 is a network visualization of interconnected keywords in research generated by VOSviewer software. This network map generated by VOSviewer illustrates the relationships between keywords in digital forensics research, showing topics that are often studied together and research trends in this field.

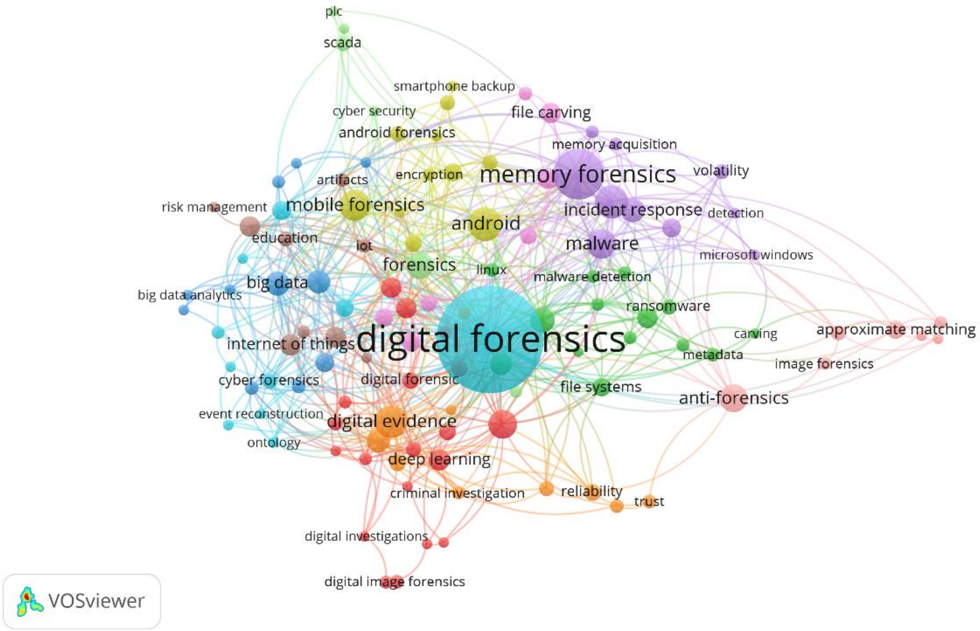

*Figure 4: Co-Occurrence Results (Network Visualization)*

At the center of the map, "digital forensics" appears as the most dominant term, connected with many other keywords. This shows that digital forensics is a major topic that covers various aspects and sub-disciplines in this research. Meanwhile, the main sub-domains are described as follows:

a) Memory Forensics and Malware Analysis
This sub-domain is located at the top right of the map. Keywords such as "memory analysis," "malware," and "memory acquisition" indicate that memory analysis and malware detection are significant focuses in digital forensics research. Terms like "volatility" and "live forensics" are also closely connected, showing the importance of memory analysis in live situations.

b) Mobile Forensics
Located at the top left, "mobile forensics" and related keywords such as "android," "iOS," and "smartphone forensics" highlight research that focuses on mobile devices. This shows that mobile device forensics is an important area, especially in the context of analyzing data from smartphones and instant messaging apps.

c) Big Data and Cybersecurity
The left part of the map shows the connection between "big data," "cybersecurity," and "IoT forensics." It shows that with the increasing volume of data and connected devices, digital forensics research also includes big data analysis and cybersecurity.

d) Digital Evidence and Digital Investigations
At the bottom of the map, keywords such as "digital evidence," "digital investigation," and "deep learning" indicate a focus on digital evidence and investigative techniques that use deep learning and artificial intelligence. This shows the trend of using advanced technologies in analyzing and processing digital evidence.

e) Anti-forensics and Approximate Matching
The bottom right section shows the focus on anti-forensic techniques and "approximate matching," which is used to hide or obscure digital traces. Research in this area aims to address the challenges posed by anti-forensic techniques.

The map also shows how the various sub-domains are connected. For example, "machine learning" is connected to many areas such as "malware analysis," "digital evidence," and "investigation," showing that machine learning techniques are increasingly important in digital forensics. Similarly, "blockchain" appears in the context of "cybersecurity" and "cloud forensics," signaling interest in distributed ledger technology for data security and forensics. Overall, this map provides a comprehensive overview of the digital forensics research landscape. It shows the various key topics, trends, and how different sub-domains interact with each other and contribute to the development of the field. The focus on mobile devices, memory analysis, big data, and anti-forensic techniques reflects the challenges and innovations being faced by researchers in their quest to develop more effective methods for investigating digital crimes.

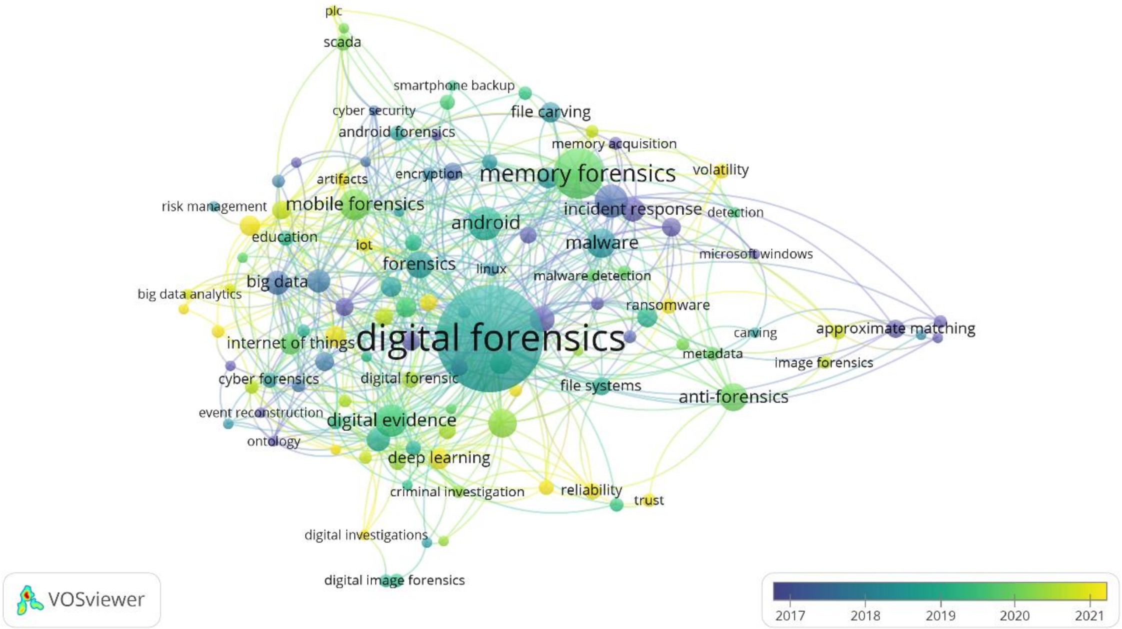

*Figure 5: Co-Occurrence Results (Overlay Visualization)*

Furthermore, Figure 5 is a visual map depicting the development of research related to digital forensic tools from 2014 to 2023. This visualization map of digital forensic topics by year provides insight into the evolution and trends of research in this field from year to year. The colors on the chart indicate the temporal distribution of research, with dark blue representing research from 2014 and yellow indicating more recent research up to 2023. Topics such as digital forensics, mobile forensics, memory forensics, and malware analysis remain a key focus over time, with research evolving to address new challenges and improve investigation techniques.

In the early years (approximately 2014 to 2016), research tended to focus on the fundamentals of digital forensics, memory forensics, and mobile forensics, with an emphasis on developing basic methodologies and tools for digital investigations. For example, early studies on Android and iOS device forensics began to receive attention, given the increased use of mobile devices. In the period from 2017 to 2019, there was an increase in topics such as malware analysis and anti-forensics. Researchers began to study more methods for detecting and analyzing malware, as well as techniques used to hide digital traces. Approximate matching began to become an area of focus, with research aimed at identifying files that have been altered to avoid detection.

From 2020 to 2022, we saw a surge in topics such as machine learning, big data analytics, and cloud forensics. The use of machine learning and big data analytics in digital forensics is becoming increasingly important, along with the need to handle ever-increasing volumes of data. Research in the field of cloud forensics is also growing, given the growing amount of data stored in cloud environments and the unique challenges that come with it. During this period, IoT forensics and drone forensics also began to receive attention, with research focusing on securing and analyzing data from Internet of Things (IoT) connected devices and drones. This reflects the increased use of these devices and the need for investigative techniques that can address their vulnerabilities.

The map also shows that research in digital forensics continues to adapt to new technologies and emerging threats, with increased use of blockchain to ensure the integrity of digital evidence and explainable AI to understand AI system decisions in forensic investigations. Overall, this visualization map illustrates the dynamic development in the field of digital forensics, with research topics constantly evolving and adapting to technological advancements and new security challenges.

### *3.4. Identification of Vacant Land in the Study*

The visualization map provided reveals a wide range of research topics in the context of digital forensics, which opens up several research opportunities for the development of digital forensics tools. One of the main opportunities lies in mobile forensics, particularly in the Android and iOS operating systems. Research can be focused on developing more effective techniques for secure data retrieval and application analysis, including methods to address encryption and data protection on smartphones as well as deleted data recovery.

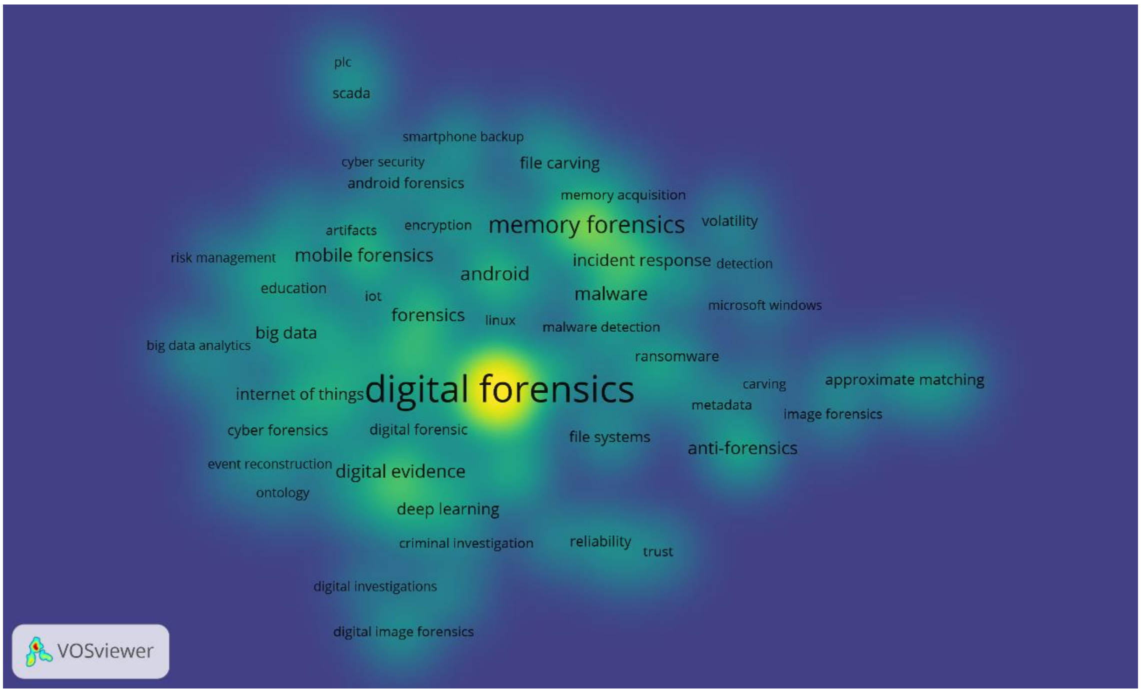

*Figure 6: Co-Occurrence Results (Density Visualization)*

In memory forensics, there is a need to improve memory acquisition and analysis methods. This includes developing techniques that support multiple platforms and environments, as well as using tools such as Volatility for faster and more accurate memory analysis to detect malware and suspicious activity. Research on anti-forensics is also highly relevant, especially in detecting and overcoming techniques used by cybercriminals to avoid detection. This could include the study of approximate matching algorithms that can recognize files or data that have been modified. Malware analysis is another important area, with a focus on developing malware detection and classification techniques using machine learning to recognize new and unknown patterns of behavior. Memory-based malware analysis also requires special attention, including detection techniques that do not rely on static signatures.

In the context of cloud forensics, research can be directed at methods of data acquisition and analysis in cloud environments, as well as the use of blockchain technology to record audit trails of digital evidence stored in the cloud, thus ensuring the integrity and authenticity of evidence. Big data analytics also offers significant research opportunities, such as the development of forensic frameworks that can efficiently handle large volumes of data and the use of big data analytics to find hidden evidence that manual analysis may have missed.

In cybersecurity, there are opportunities to focus on Internet of Things (IoT) device forensics, including the collection and analysis of data from various interconnected devices, as well as drone forensics involving the analysis of navigation and communication data. Furthermore, the use of machine learning and deep learning in digital investigations offers great potential for automating forensic analysis, including the classification of digital evidence and prediction of suspicious activity. Research on explainable AI is also important to enable investigators to understand and trust the results of AI analysis. Finally, the issue of "privacy" is on the map, but further research is needed to address the ethical and privacy challenges that arise in digital forensic investigations. This includes developing frameworks to ensure that digital forensics practices comply with applicable privacy laws and ethical standards.

By identifying these areas, researchers can direct their efforts toward filling gaps in the literature and developing innovative solutions that can strengthen the field of digital forensics as a whole. These opportunities show how the various sub-topics in digital forensics can be explored to develop more sophisticated, efficient, and accurate forensic tools to address evolving digital security challenges.

## 4. CONCLUSION

This study aimed to evaluate the evolution of digital forensic tools research over the past decade, identify key trends and contributions, and uncover promising opportunities for future exploration. By conducting a bibliometric analysis of 698 Scopus-indexed articles published from 2014 to 2023 in the business, management, and accounting domains, the research achieved its purpose of providing a comprehensive overview of the field. The findings demonstrate a growing body of work in digital forensics, with significant contributions from prominent researchers like Frank Breitinger and Ibrahim Baggili, who have been central to advancements in mobile forensics, malware analysis, and anti-forensics.

The study also identified notable research gaps, such as the need for more robust techniques in memory forensics, improved methods for data acquisition in cloud environments, and innovative applications of emerging technologies like blockchain and explainable AI. Ethical and privacy challenges in forensic investigations were highlighted as critical areas requiring further exploration to ensure legal compliance and moral accountability in the field.

By addressing these gaps and extending research to other databases and disciplines, future studies can enhance the reliability, efficiency, and ethical standards of digital forensic tools. Although limited to the ScienceDirect database and a specific domain focus, this study provides a valuable foundation for researchers, practitioners, and policymakers to advance digital forensic practices, tackle evolving digital security challenges, and foster interdisciplinary collaboration to drive innovation in the field.

## 5. RECOMMENDATION

The main limitation of this study is the use of only one data source, ScienceDirect, as well as limiting the time span of the study to the last ten years, from 2014 to 2023. In addition, the subject of this research is only in the context of business, management, and accounting. This could potentially result in a lack of thorough representation of the latest developments in digital forensic tools. Therefore, future research is expected to expand its scope by considering the use of other relevant data sources, such as Web of Science, IEEE Xplore, PubMed, arXiv, or SpringerLink, using other subject areas such as computer science or social science, and extending the research time span to cover a wider period. This will allow researchers to gain a more comprehensive understanding of the developments in the utilization of machine learning technology in fraud detection, as well as ensure that no contributions are overlooked.

## REFERENCES

[1] S. S. Alsemairi, “The Role of Digital Technologies in Combating Cyber-Trafficking in Persons Crimes,” *Comput. Inf. Sci.*, vol. 16, no. 1, pp. 49–64, 2023, doi: 10.5539/cis.v16n1p49.

[2] A. R. Javed, W. Ahmed, M. Alazab, Z. Jalil, K. Kifayat, and T. R. Gadekallu, “A Comprehensive Survey on Computer Forensics: State-of-the-Art, Tools, Techniques, Challenges, and Future Directions,” *IEEE Access*, vol. 10, no. 1, pp. 11065–11089, 2022, doi: 10.1109/ACCESS.2022.3142508.

[3] E. K. Brown, “Digital Forensic and Distributed Evidence,” *Res. Nexus IT, Law, Cyber Secur. Forensics*, vol. 1, no. 1, pp. 357–362, 2022, doi: 10.22624/aims/crp-bk3-p57.

[4] I. Riadi, A. Yudhana, and Galih Pramuja Inngam Fanani, “Comparative Analysis of Forensic Software on Android-based MiChat using ACPO and DFRWS Framework,” *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 7, no. 2, pp. 286–292, 2023, doi: 10.29207/resti.v7i2.4547.

[5] I. Riadi, H. Herman, and N. H. Siregar, “Mobile Forensic of Vaccine Hoaxes on Signal Messenger using DFRWS Framework,” *MATRIK J. Manajemen, Tek. Inform. dan Rekayasa Komput.*, vol. 21, no. 3, pp. 489–502, 2022, doi: 10.30812/matrik.v21i3.1620.

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

[7] G. N. Samy *et al.*, “Proposed proactive digital forensic approach for cloud computing environment,” *Int. J. Eng. Technol.*, vol. 7, no. 4.15, pp. 12–15, 2018, doi: 10.14419/ijet.v7i4.15.21362.

[8] A. A. Khan, A. A. Shaikh, A. A. Laghari, and M. M. Rind, “Cloud forensics and digital ledger investigation: a new era of forensics investigation,” *Int. J. Electron. Secur. Digit. Forensics*, vol. 15, no. 1, pp. 1–23, 2023, doi: 10.1504/IJESDF.2023.10045851.

[9] R. Kumar, K. S. Kakade, M. Priscilla, and B. V. S. Krishna, “An effective digital forensic paradigm for cloud computing criminal investigation,” *Int. J. Electron. Secur. Digit. Forensics*, vol. 15, no. 6, pp. 655–664, 2023, doi: 10.1504/IJESDF.2023.133966.

[10] B. Kaur, K. Sood, and S. Grima, “A systematic review on forensic accounting and its contribution towards fraud detection and prevention,” *J. Financ. Regul. Compliance*, vol. 31, no. 1, pp. 60–95, 2023, doi: 10.1108/JFRC-02-2022-0015.

[11] H. Yarovenko and M. Rogkova, “Dynamic and bibliometric analysis of terms identifying the combating financial and cyber fraud system,” *Financ. Mark. Institutions Risks*, vol. 6, no. 3, pp. 93–104, 2022, doi: 10.21272/fmir.6(3).93-104.2022.

[12] M. Wundram, F. C. Freiling, and C. Moch, "Anti-forensics: The next step in digital forensics tool testing," *Proc. - 7th Int. Conf. IT Secur. Incid. Manag. IT Forensics, IMF 2013*, vol. 7, no. 1, pp. 83–97, 2013, doi: 10.1109/IMF.2013.17.

[13] M. Gengenbach, A. Chassanoff, and P. Olsen, "Integrating digital forensics into born-digital workflows: The BitCurator project," *Proceedings of the ASIST Annual Meeting*, vol. 49, no. 1. pp. 1–4, 2012. doi: 10.1002/meet.14504901343.

[14] V. K. Devendran, H. Shahriar, and V. Clincy, "A Comparative Study of Email Forensic Tools," *J. Inf. Secur.*, vol. 06, no. 02, pp. 111–117, 2015, doi: 10.4236/jis.2015.62012.

[15] Y. Yannikos and C. Winter, "Model-based generation of synthetic disk images for digital forensic tool testing," *Proc. - 2013 Int. Conf. Availability, Reliab. Secur. ARES 2013*, vol. 1, no. 1, pp. 498–505, 2013, doi: 10.1109/ARES.2013.65.

[16] J. L. Bierstaker, R. G. Brody, and C. Pacini, "Accountants' perceptions regarding fraud detection and prevention methods," *Manag. Audit. J.*, vol. 21, no. 5, pp. 520–535, 2006, doi: 10.1108/02686900610667283.

[17] A. Parveen, Z. H. Khan, and S. N. Ahmad, "Classification and evaluation of digital forensic tools," *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 18, no. 6, pp. 3096–3106, 2020, doi: 10.12928/TELKOMNIKA.v18i6.15295.

[18] O. E. Akinbowale, H. E. Klingelhöfer, and M. F. Zerihun, "An innovative approach in combating economic crime using forensic accounting techniques," *J. Financ. Crime*, vol. 27, no. 4, pp. 1253–1271, 2020, doi: 10.1108/JFC-04-2020-0053.

[19] H. Adamu, A. A. Ahmad, A. Hassan, and S. B. Gambasha, "Web Browser Forensic Tools: Autopsy, BHE and Net Analysis," *Int. J. Res. Innov. Appl. Sci.*, vol. 6, no. 6, pp. 56–61, 2021, doi: 10.51584/ijrias.2021.6506.

[20] S. Subektiningsih and D. Hariyadi, "The Role of Digital Forensic Experts in Cybercrime Investigations in Indonesia Based on The Scopus Research Index," *Build. Informatics, Technol. Sci.*, vol. 4, no. 3, pp. 1665–1670, 2022, doi: 10.47065/bits.v4i3.2638.

[21] P. H. Rughani, "Artificial Intelligence Based Digital Forensics Framework," *Int. J. Adv. Res. Comput. Sci.*, vol. 8, no. 8, pp. 10–14, 2017, doi: 10.26483/ijarcs.v8i8.4571.

[22] Y. Guo and J. Slay, "Data Recovery Function Testing for Digital Forensic Tools," *Adv. Digit. Forensics*, vol. 6, no. 1, pp. 297–311, 2010.

[23] S. Karyana, O. Sumarna, and A. Setiawan, "Bibliometric Computational Mapping Analysis of Publications on Computational Thinking in Science Education using VOSviewer," *J. Adv. Res. Appl. Sci. Eng. Technol. J.*, vol. 58, no. 2, pp. 70–84, 2024.

[24] H. N. Genc, N. Kocak, N. Bibliometric, H. N. Genc, and N. Kocak, "Bibliometric Analysis of Studies on the Artificial Intelligence in Science Education with VOSviewer," *J. Educ. Sci. Environ. Heal.*, vol. 10, no. 4, pp. 183–195, 2024.

[25] Z. Guofang, M. S. Rasul, and M. Omar, “A Bibliometric Analysis of Publications on University- Industry Collaboration Using VOSviewer and R- biblioshiny,” *Multidiscip. J. Educ. Soc. Technol. Sci.*, vol. 11, no. 2, pp. 26–50, 2024.

[26] D. Moher, A. Liberati, J. Tetzlaff, and D. G. Altman, “Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement,” *BMJ*, vol. 339, no. 7716, pp. 332–336, 2009, doi: 10.1136/bmj.b2535.

[27] A. Budiani and S. Sopiah, "Green human resource management: A systematic literature review (SLR) and bibliometric analysis," *Jurnal Syntax Fusion*, vol. 2, no. 11, pp. 818-832, 2022.

[28] A. Zaskia, "Intensi berwirausaha: Analisis bibliometrik," *OIKOS: J. Kajian Pendidik. Ekonomi dan Ilmu Ekonomi*, vol. 7, no. 1, pp. 136-152, 2023.