

Mobile forensics tools and techniques for digital crime investigation: a comprehensive review

Tole Sutikno

Faculty of Industrial Technology, Universitas Ahmad Dahlan, Yogyakarta, Indonesia

Article Info

Article history:

Received May 30, 2024

Revised Jul 7, 2024

Accepted Jul 15, 2024

Keywords:

Data extraction

Digital crime investigation

Encryption

Forensic software tools

Mobile forensics

Mobile phone

ABSTRACT

Extracting and analyzing data from smartphones, IoT devices, and drones is crucial for conducting digital crime investigations. Effective cyberattack mitigation necessitates the use of advanced Android mobile forensics techniques. The investigation necessitates proficiency in manual, logical, hex dump, chip-off, and microread methodologies. This paper provides a comprehensive overview of Android mobile forensics tools and techniques for digital crime investigation, as well as their use in gathering and analyzing evidence. Forensic software tools like Cellebrite UFED, Oxygen Forensic Detective, XRY by MSAB, Magnet AXIOM, SPF Pro by SalvationDATA, MOBILedit Forensic Express, and EnCase Forensic employ both physical and logical techniques to retrieve data from mobile devices. These advanced tools offer a structured approach to tackling digital crimes effectively. We compare dependability, speed, compatibility, data recovery accuracy, and reporting. Mobile-network forensics ensures data acquisition, decryption, and analysis success. Conclusions show that Android mobile forensics tools for digital crime investigations are diverse and have different capabilities. Mobile forensics software offers complete solutions, but new data storage and encryption methods require constant development. The continuous evolution of forensic software tools and a comprehensive tool classification system could further enhance digital crime investigation capabilities.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Tole Sutikno

Faculty of Industrial Technology, Universitas Ahmad Dahlan

4th Campus, Main Buliding, 6th Floor, Yogyakarta, Indonesia

Email: tole@te.uad.ac.id

1. INTRODUCTION

In the field of digital crime investigation, the use of mobile forensics tools and techniques is crucial for acquiring and analyzing evidence [1]–[5]. Various sophisticated tools, such as Cellebrite UFED [6], [7], Oxygen Forensic Detective [6], [8], and XRY by MSAB [8], offer a wide range of features and functionalities to extract data from different mobile platforms. These tools play a significant role in accessing critical data from smartphones, IoT devices, and even drones, allowing investigators to collect valuable evidence. The evolution of forensic software tools has led to the development of new techniques like physical and logical extraction, which utilize different connections such as JTAG, cables, Bluetooth, infrared, and more. With tools, forensic experts have a plethora of options to choose from depending on the specific requirements of the investigation [9]–[13].

In recent years, the field of mobile forensics has seen significant growth with the proliferation of Android devices. Forensic investigators face numerous challenges due to the diversity of device models and operating system versions across the Android ecosystem. To tackle this complexity, researchers have developed a multitude of forensic tools and techniques to extract and analyze digital evidence from Android

devices. These tools vary in their capabilities, usability, and effectiveness in different investigative scenarios. Also, these tools are categorized by techniques like manual extraction, logical extraction, hex dump, chip-off, and microread, which shows the variety of ways that forensic experts get data from Android devices. As the landscape of digital crime continues to evolve, the need for reliable and efficient Android mobile forensics tools becomes increasingly crucial for successful investigations [8], [12]–[24].

Using advanced forensic tools and techniques is crucial in digital crime investigation. These tools play a pivotal role in acquiring, analyzing, and interpreting digital evidence from various mobile platforms, including smartphones, IoT devices, and drones. The array of forensic tools available, such as Cellebrite UFED, Oxygen Forensic Detective, and XRY by MSAB, provide investigators with the means to access critical data in an efficient and effective manner. Moreover, the constant evolution of forensic software tools introduces new techniques for extracting data from cellular devices, including physical and logical extraction methods. The classification system for these tools, which includes manual extraction, hex dump, chip-off, and microread, offers investigators a structured approach to digital crime investigation. By leveraging these tools and techniques, investigators can navigate the complex landscape of digital crime with precision and thoroughness [1]–[4], [7], [10], [12], [20], [25]–[31].

Due to the growing use of smartphones in criminal activities, forensic software tools for Android mobile devices are critical in digital crime investigations. These tools provide a wide range of functionalities for efficiently collecting and analyzing data from various mobile platforms. The capabilities of the previously mentioned tools vary, ranging from simple data extraction to more advanced techniques such as JTAG physical extraction and logical extraction via various connections. According to research, these tools play an important role in accessing critical data from a variety of devices, including smartphones, IoT devices, and drones, thereby aiding the investigation process. These tools provide a comprehensive approach to digital forensics and evidence collection on Android mobile devices by using techniques such as manual extraction, logical extraction, hex dump, chip-off, and microread [18], [32]–[41].

Forensic software tools are constantly evolving to meet the demands of extracting data from a variety of mobile devices. These tools, such as Cellebrite UFED and Oxygen Forensic Detective, offer a range of features and functionalities tailored to different use cases and scenarios. The comprehensive review of Android mobile forensics tools and techniques for digital crime investigation aims to provide a detailed analysis of the purpose and scope of these tools in acquiring and analyzing evidence from smartphones, cloud services, and IoT devices. By examining the pros and cons of tools like XRY by MSAB and Magnet AXIOM, researchers can better understand the capabilities and limitations of each tool in different forensic scenarios. This review will also consider the classification system of forensic tools, including manual extraction, logical extraction, hex dump, chip-off, and microread, to provide a comprehensive overview of the techniques used in the field [18], [19], [33], [34], [38].

In the realm of digital crime investigation, the significance of comparing tools and techniques manifests itself in the efficacy and dependability of obtaining critical evidence for court proceedings. According to Groß [42], the performance differences among forensic tools such as UltData Android, Wondershare Dr. Fone, and EaseUs Mobisaver highlight the importance of meticulous comparison to determine the most proficient data restoration capabilities. Furthermore, as stated in [43], addressing anti-forensic challenges in Android phones necessitates a thorough understanding of the tools and methods used in mobile forensics. Investigators can navigate complexities such as encoded files and data tampering by examining the capabilities, limitations, and advancements in forensic software tools, thereby enhancing the integrity and effectiveness of digital evidence collection. Thus, comprehensive tool and technique evaluation is critical for improving the investigative process and ensuring the robustness of digital forensic practices [12].

Recent advances in digital technology have greatly expanded the capabilities of mobile phone data analysis in a variety of fields, including criminology and urban sensing applications. The use of mobile phone data allows researchers to delve into human communication behaviors and mobility patterns, serving as a critical resource for studying and predicting criminal activities, detecting suspicious behaviors, and understanding urban population dynamics [10], [17], [24], [25], [27], [28], [36], [38], [44]. This comprehensive review explores the use of mobile phone data in crime prevention and mobility analysis. It highlights the growing focus on human mobility patterns over communication behaviors due to privacy and data collection concerns. The study emphasizes the importance of advanced tools like social network analysis and correlation analysis in detecting spatial-temporal crime patterns and identifying criminal networks in urban settings. It also discusses Android mobile forensics tools and techniques, such as Cellebrite UFED, Oxygen Forensic Detective, and XRY by MSAB, which are designed to acquire and analyze evidence from various mobile platforms. These tools are compatible with smartphones, cloud services, and IoT devices, and enable data extraction from burner phones, feature phones, smartphones, IoT devices, and drones. The review emphasizes the need to stay updated on the latest tools and techniques to effectively investigate digital crimes.

2. ANDROID MOBILE FORENSICS TOOLS

The advancement of forensic software tools plays a crucial role in the field of digital forensics, particularly in mobile device investigations. The acquisition, analysis, and use of digital evidence in criminal investigations have undergone a revolution thanks to these tools. The wide range of tools available, such as Cellebrite UFED, Oxygen Forensic Detective, and XRY by MSAB, provide investigators with various options for extracting and examining data from different mobile platforms. Techniques like physical and logical extraction, as well as the classification system of tools, further enhance the efficiency and accuracy of digital crime investigations. By constantly developing new techniques and staying ahead of technological advancements, forensic software tools contribute significantly to the field of digital forensics, ensuring that investigators have the necessary resources to uncover vital evidence from a diverse array of mobile devices.

Technological advancements play a significant role in combating digital crimes in the realm of Android mobile forensics tools. As highlighted by [42], the use of smartphones as a medium for criminal activities necessitates robust forensic tools to retrieve deleted data and secure digital evidence that is critical for legal proceedings. The comparative analysis revealed that UltData Android excels in data restoration, aligning with the evolving demands of digital investigations. Furthermore, Bhushan [43] emphasizes the challenges posed by anti-forensic issues on mobile devices, accentuating the need for continuous improvements in data acquisition and forensic methodologies. The integration of SVM machine learning techniques emerges as a potential solution to address file encoding complexities, showcasing the innovation within the field. These insights underscore the dynamic landscape of Android mobile forensics tools, emphasizing the pivotal role they play in advancing digital crime investigations.

2.1. Cellebrite UFED

In the realm of mobile forensics tools, Cellebrite UFED stands out as a leading solution for acquiring and analyzing digital evidence from a wide range of mobile platforms. This powerful tool offers a comprehensive suite of features and functionalities that enable investigators to conduct thorough forensic examinations on smartphones, IoT devices, and drones. Cellebrite UFED, in conjunction with other tools like Oxygen Forensic Detective and XRY by MSAB, plays a crucial role in digital crime investigations by granting access to crucial data that aids in constructing a case against the perpetrators. The versatility and reliability of Cellebrite UFED make it a valuable asset in the arsenal of forensic professionals, allowing them to delve deep into the digital footprint left behind by suspects. Additionally, the continuous development and improvement of forensic software tools, including Cellebrite UFED, highlight the ongoing efforts to stay at the forefront of digital forensic technology.

2.2. Oxygen forensic detective

Furthermore, in the realm of mobile forensic tools, Oxygen Forensic Detective stands out as a comprehensive and versatile option for digital crime investigation. With its advanced features and capabilities, Oxygen Forensic Detective is able to extract and analyze data from a wide range of mobile devices, including smartphones, feature phones, IoT devices, and drones. The tool offers a user-friendly interface coupled with powerful data parsing and decoding capabilities, making it an essential asset for forensic investigators. Additionally, Oxygen Forensic Detective provides support for both physical and logical extraction methods, enabling investigators to access critical data through various means such as JTAG, cable connections, Bluetooth, and more. Its classification system covers manual extraction, logical extraction, hex dump, chip-off, and microread techniques, further solidifying its status as a top-tier tool in the field of mobile forensics [45].

2.3. XRY by MSAB

When considering the various forensic tools available for mobile platform analysis, XRY by MSAB stands out as a comprehensive solution for digital crime investigation. XRY offers a range of key features and functionalities that cater to different use cases and scenarios in the field. It allows for the easy acquisition and analysis of critical data from a wide array of mobile devices, including burner phones, feature phones, smartphones, IoT devices, and drones. The tool is constantly evolving to keep up with the changing landscape of mobile technology, offering both physical and logical extraction methods. By utilizing JTAG, cable connections, Bluetooth, infrared, or other means, XRY ensures that investigators have multiple options for extracting data efficiently. In the realm of mobile forensics, XRY by MSAB remains a reliable and robust software tool that aids in the extraction and analysis of data from various devices [46].

2.4. Magnet AXIOM

Forensic software tools play a vital role in acquiring and analyzing evidence from mobile devices in digital crime investigations. Among the myriad of tools available, Magnet AXIOM stands out as a comprehensive solution that offers a range of features and functionalities for investigators. These include data

acquisition, analysis, and reporting capabilities for various mobile platforms. The tool enables the extraction of critical data from smartphones, cloud storage, and IoT devices, providing valuable insights into digital evidence. We continuously update Magnet AXIOM with new techniques to ensure reliable data extraction, supporting both physical and logical extraction methods. Its classification system categorizes tools based on manual extraction, logical extraction, hex dump, chip-off, and microread techniques, allowing investigators to choose the most suitable approach for their specific case. With its user-friendly interface and powerful capabilities, Magnet AXIOM is a valuable asset for digital forensic investigators.

2.5. SPF Pro by SalvationDATA

Mobile forensic tools play a vital role in digital crime investigations because they enable forensic experts to gather and analyze evidence from various devices. One such tool, SPF Pro by SalvationDATA, offers advanced features for extracting and processing data from smartphones, cloud storage, and IoT devices. SPF Pro is a versatile tool that supports both physical and logical extraction methods, allowing users to access data through JTAG, cable connections, Bluetooth, infrared, or other means. In a comparative analysis of mobile forensic tools, SPF Pro stands out for its comprehensive functionality and effectiveness in handling a wide range of devices. This tool, along with others like Cellebrite UFED, XRY by MSAB, and MOBILedit Forensic Express, contributes significantly to the successful investigation and prosecution of digital crimes. Future research should focus on evaluating the specific capabilities and limitations of SPF Pro when compared to other leading tools in the field [45].

2.6. MOBILedit Forensic Express

In the realm of mobile forensic tools, MOBILedit Forensic Express stands out as a comprehensive and powerful solution for acquiring and analyzing data from a wide range of mobile devices. This tool offers a variety of features and functionalities that cater to the needs of digital crime investigators. MOBILedit Forensic Express is known for its user-friendly interface, advanced data extraction capabilities, and compatibility with various mobile platforms. It enables investigators to extract data through both physical and logical extraction techniques, providing a versatile approach to digital evidence collection. Additionally, MOBILedit Forensic Express undergoes constant updates to integrate new techniques for data extraction from various cellular devices, guaranteeing investigators the latest tools and methods in mobile forensics. Its classification system includes manual extraction, logical extraction, hex dump, chip-off, and microread, making it a versatile tool for digital crime investigations [21].

2.7. EnCase Forensic

EnCase Forensic is one of the most prominent mobile forensics tools. This comprehensive software offers a wide array of features and functionalities that cater to the needs of digital crime investigators. EnCase Forensic is known for its robust capabilities in both acquiring and analyzing evidence from various mobile platforms. With its user-friendly interface and powerful data extraction algorithms, EnCase Forensic enables investigators to delve deep into the data stored in smartphones, IoT devices, and even drones. The tool's versatility allows for easy access to critical data from a diverse range of devices, including burner phones and feature phones. Through techniques such as physical and logical extraction, EnCase Forensic stands out as a valuable asset in the investigative process. Its classification within the tools system-Manual extraction, Logical extraction, Hex dump, Chip-off, and Microread-further highlights its importance in the digital crime investigation landscape [47].

3. TECHNIQUES FOR ANDROID MOBILE FORENSICS

Figure 1 illustrates the leveling pyramid for the mobile device forensics tool class. In the realm of digital forensics, the need for advanced techniques in Android mobile forensics is paramount in combating the escalating threats of cyberattacks. Understanding the complex landscape of mobile device investigation necessitates a thorough examination of the available tools and methodologies. The thorough review of digital forensic tools builds on what other studies [26] have found and sheds light on the most important parts of investigation processes, judging performance, and the importance of domain-specific issues in Android mobile forensics [48]. By looking into the tool classification system, which includes manual extraction, logical extraction, hex dump, chip-off, and microread techniques, forensic experts can use a variety of strategies to get important data from different mobile platforms. In the ever-changing digital landscape, this strategic approach is critical to achieving comprehensive and effective digital crime investigations.

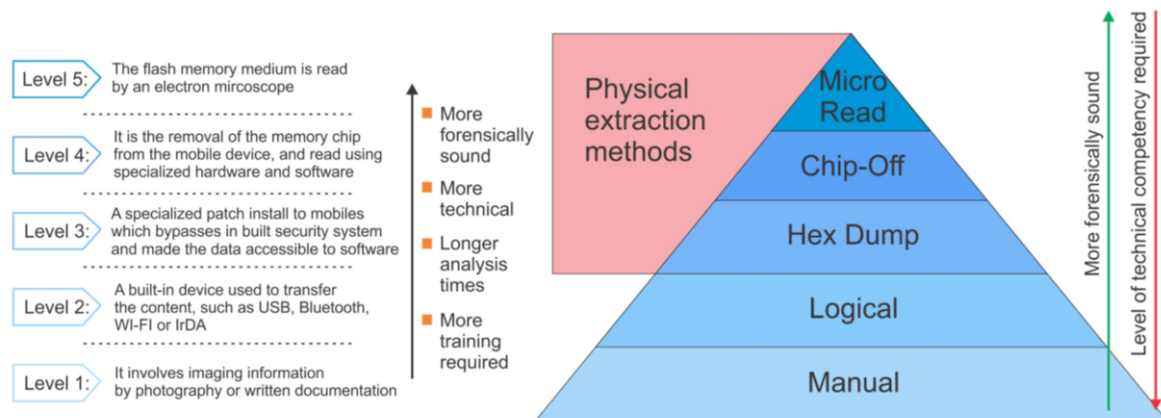


Figure 1. The leveling pyramid of the mobile device forensics tool classification

3.1. Manual extraction

In the realm of mobile forensics, manual extraction serves as a vital component in the process of acquiring digital evidence. This method involves physically accessing the device and extracting data manually, which can be a time-consuming but crucial aspect of forensic investigations. Manual extraction can provide a deeper level of access to the device compared to automated tools, allowing forensic experts to recover data that may have been deleted or encrypted. However, manual extraction requires specialized knowledge and expertise to ensure the integrity of the evidence and prevent any unintentional alterations to the data. According to, manual extraction remains a valuable technique in the arsenal of forensic tools, particularly in cases where automated methods may not be sufficient to recover critical information. Additionally, Hoog [21] underscores the importance of considering manual extraction alongside other tools and techniques to ensure a comprehensive approach to digital crime investigation.

3.2. Logical extraction

Forensic software tools are constantly developing new techniques for extracting data from multiple cellular devices. The two most common techniques are physical and logical extraction. JTAG or cable connections facilitate physical extraction, while Bluetooth, infrared, or cable connections facilitate logical extraction. Logical extraction is a crucial method in digital forensics as it enables investigators to access data without altering the original content. This technique allows for the extraction of data stored in the device's memory, files, databases, and applications such as call logs, text messages, photos, and app data. Logical extraction provides a non-intrusive method of acquiring evidence and is often preferred in situations where physical extraction is not possible or desirable. The tools classified under logical extraction offer a non-intrusive way of acquiring evidence, ensuring that crucial data is obtained efficiently and accurately during forensic analysis. Additionally, this method can be especially useful when dealing with sensitive and sophisticated digital devices, further enhancing its significance in the realm of mobile forensics. However, it is important to note that logical extraction may not capture all the data present on a device compared to physical extraction methods. Researchers have indicated that logical extraction is fundamental in digital crime investigation because of its non-invasive nature [21].

3.3. Physical extraction (Hex dump)

Forensic software tools are constantly evolving to meet the demands of digital crime investigations. These tools employ various techniques for extracting data from mobile devices, with physical and logical extraction being the most common methods. Physical extraction involves connecting the device via JTAG or cable to retrieve data, while logical extraction utilizes wireless technologies like Bluetooth or infrared. A key component of the forensic process is the hex dump, which provides a detailed representation of a device's memory contents. This technique is instrumental in uncovering valuable information during investigations, such as deleted files or hidden data. A hex dump, also called physical extraction, extracts the raw image in binary format from the mobile device. By utilizing hex dumps, forensic analysts can decode and interpret complex data structures to reconstruct events and timelines, ultimately aiding in the resolution of digital crimes. The classification system for forensic tools includes manual extraction, logical extraction, hex dump, chip-off, and microread methods, each offering unique capabilities for acquiring and analyzing mobile device data [18].

In the realm of Android mobile forensics, the process of physical extraction plays a pivotal role in retrieving crucial data for digital crime investigations. As smartphones emerge as vast repositories of user profile data, the challenges in acquiring and analyzing this information become increasingly complex. With the evolution of mobile smart phone technology, especially in Android devices, the use of virtual Android phones through tools like Genymotion Emulator offers a non-intrusive method for forensic analysis, eliminating the need for physical procurement of devices. The integration of open-source tools in this virtual environment allows researchers to focus on extracting forensic artifacts without the necessity of rooting or bypassing phone security. This approach not only enhances the efficiency of the forensic analysis but also enables researchers to delve into developing innovative techniques for maximizing artifact extraction, aligning with the continuous advancements in forensic software tools for comprehensive digital evidence acquisition and analysis.

3.4. Chip-off

In the realm of mobile forensics, the 'Chip-off' technique stands out as a complex yet valuable method for extracting data from devices. This technique involves physically removing the memory chip from the mobile device and accessing the data directly. By bypassing the device's security mechanisms through this invasive procedure, examiners can potentially recover deleted or encrypted data that would otherwise be inaccessible. However, the 'Chip-off' technique requires specialized equipment, skills, and meticulous handling to prevent damage to the memory chip and ensure the integrity of the extracted data. While this method is considered a last resort due to its invasive nature and potential risks, it remains a powerful tool in the forensic examiner's arsenal for tackling cases where traditional extraction methods prove ineffective. As such, the 'Chip-off' technique represents a crucial aspect of the forensic toolkit, offering a unique approach to digital crime investigation.

3.5. Microread

Some of the advanced mobile forensics tools utilize a technique called Microread, which involves the analysis of tiny fragments of data at a microscopic level to extract critical information from mobile devices. Microread enables forensic investigators to delve deep into the intricate details of a device's memory and storage components, allowing for the recovery of deleted files, hidden data, and other digital evidence that may have been overlooked through traditional extraction methods. This cutting-edge technique has revolutionized the field of mobile forensics by providing investigators with a powerful tool to uncover valuable insights that can strengthen their case and contribute to the successful resolution of digital crimes. By incorporating Microread into their investigative processes, forensic experts can enhance the efficiency and effectiveness of their data extraction and analysis efforts, ultimately leading to more robust and conclusive findings in digital crime investigations.

4. COMPARATIVE ANALYSIS OF ANDROID MOBILE FORENSICS TOOLS AND TECHNIQUES

Forensic software tools are constantly developing new techniques for extracting data from multiple cellular devices. The two most common techniques are physical and logical extraction. JTAG or cable connections facilitate physical extraction, while Bluetooth, infrared, or cable connections facilitate logical extraction. When comparing Android mobile forensics tools and techniques, it is essential to consider factors such as reliability, speed, ease of use, compatibility with different android versions, data recovery accuracy, and reporting capabilities. Cellebrite UFED and Oxygen Forensic Detective are among the leading tools in the field, known for their comprehensive capabilities in acquiring and analyzing data from Android devices. However, further comparative analysis is needed to determine which tools and techniques are the most suitable for specific forensic investigation scenarios. Additionally, tools are categorized into manual extraction, logical extraction, hex dump, chip-off, and microread methods based on their functionality and approach to data acquisition and analysis [21].

4.1. Key features and functionalities

One of the key aspects of mobile forensic tools is their ability to extract and analyze data from a wide range of mobile devices, including smartphones, IoT devices, and drones. These tools, such as Cellebrite UFED and Oxygen Forensic Detective, offer various features and functionalities tailored to different use cases and scenarios. For instance, some tools specialize in data extraction from cloud services, while others focus on data from IoT devices. Despite the diversity in their functionalities, these tools share common techniques, such as physical and logical extraction methods. Physical extraction typically involves JTAG or cable connections, while logical extraction can be achieved through Bluetooth, infrared, or cable connections. The classification

system of these tools includes manual extraction, logical extraction, hex dump, chip-off, and microread techniques, highlighting the comprehensive range of capabilities offered by modern forensic software tools. These features enable investigators to access and analyze critical data efficiently, making them indispensable in digital crime investigations [18].

4.2. Use cases and scenarios

One crucial aspect to consider when comparing Android mobile forensics tools is the use cases and scenarios in which these tools can be applied. According to experts in the field, understanding the specific contexts in which these tools are effective is essential for successful digital crime investigations. Different tools may excel in acquiring and analyzing data from different types of mobile devices, such as smartphones, feature phones, IoT devices, and even drones. By examining the use cases and scenarios provided by each tool, investigators can choose the most suitable option for their specific requirements. For example, some tools may specialize in cloud data extraction, while others may focus on physical extraction from a wide range of devices. Additionally, considering the various classification systems for these tools, including manual extraction, logical extraction, hex dump, chip-off, and microread, can further inform investigators on the best tool for their investigative needs [45]. These insights into use cases and scenarios are crucial in guiding the selection and deployment of Android mobile forensics tools for digital crime investigations in an ever-evolving technological landscape.

4.3. Pros and cons

One of the major advantages of utilizing Android mobile forensics tools for digital crime investigations is the wide range of available software options, each offering unique features and capabilities tailored to different investigative needs. These tools can efficiently extract data from a variety of mobile devices, including smartphones and IoT devices, enabling investigators to analyze critical information for solving criminal cases. However, a potential drawback of using these tools is the constant need to keep up with the evolving technology landscape to ensure compatibility with the latest devices and operating systems. Additionally, the complexity of some tools may require specialized training for investigators to effectively utilize them in forensic examinations. Despite these challenges, the benefits of using Android mobile forensics tools, such as quick access to vital data and comprehensive analysis capabilities, outweigh the drawbacks, making them indispensable resources for digital crime investigations [21].

4.4. Data extraction from smartphones

The field of digital forensics is constantly evolving to keep pace with the rapidly changing landscape of mobile technology. Various forensic tools are available for acquiring and analyzing evidence from a wide range of mobile platforms. These tools play a crucial role in the extraction and analysis of data from smartphones, cloud services, and IoT devices. Some popular tools include Cellebrite UFED, Oxygen Forensic Detective, and XRY by MSAB. These tools utilize different techniques such as physical and logical extractions to access data from mobile devices. The classification system for these tools includes manual extraction, logical extraction, hex dump, chip-off, and microread methods. By employing these sophisticated tools and techniques, forensic experts can effectively extract vital information from different types of mobile devices, aiding in the investigation and prosecution of digital crimes [21].

4.5. Data extraction from cloud services

Forensic software tools are constantly developing new techniques for extracting data from multiple cellular devices. The two most common techniques are physical and logical extraction. JTAG or cable connections facilitate physical extraction, while Bluetooth, infrared, or cable connections facilitate logical extraction. Various forensic tools like Cellebrite UFED and Oxygen Forensic Detective are equipped with capabilities for extracting crucial data from smartphones and cloud services. Data extraction from cloud services poses unique challenges due to the distributed nature of cloud computing and the encryption protocols used to secure data transmission. Tools such as MOBILedit Forensic Express and EnCase Forensic employ advanced algorithms to overcome these challenges and extract data efficiently from cloud servers. The classification system for these tools includes manual extraction, logical extraction, hex dump, chip-off, and microread methods, providing investigators with a comprehensive suite of options for data retrieval [21].

4.6. Data extraction from IoT devices

When it comes to digital crime investigations involving IoT devices, one crucial aspect is the data extraction process. Forensic software tools play a pivotal role in acquiring and analyzing evidence from these devices, alongside mobile platforms. These tools, such as Cellebrite UFED and XRY by MSAB, offer various features and functionalities that cater to different use cases and scenarios. They enable professionals to access and analyze critical data from a wide range of devices, including smartphones and IoT devices. In this context,

the techniques used for data extraction, such as physical and logical extraction, are fundamental. Physical extraction methods involving JTAG or cable connections are typically used for in-depth retrieval, while logical extraction methods often rely on wireless or cable connections. Additionally, tools are classified into categories like manual extraction, logical extraction, hex dump, chip-off, and microread, showcasing the diversity of approaches available for extracting crucial data from IoT devices.

4.7. Comparison of data extraction methods

Forensic software tools are constantly developing new techniques for extracting data from multiple cellular devices. The two most common techniques are physical and logical extraction. JTAG or cable connections facilitate physical extraction, while Bluetooth, infrared, or cable connections facilitate logical extraction. Various forensic tools are available for acquiring and analyzing evidence from various mobile platforms, such as Cellebrite UFED, Oxygen Forensic Detective, XRY by MSAB, Magnet AXIOM, SPF Pro by SalvationDATA, MOBILedit Forensic Express, EnCase Forensic, Andriller, GrayKey, Belkasoft, Evidence Center X, MSAB XRY, Hancm MD-NEXThot icon, and Dr. Fone. These tools take into account key features and functionalities, use cases and scenarios, pros and cons, and data from smartphones, cloud, and IoT devices. These tools facilitate the easy access, analysis, and action of critical data from thousands of mobile devices, including burner phones, feature phones, smartphones, IoT devices, and drones. The tools are classified into Manual extraction, Logical extraction, Hex dump, Chip-off, and Microread, showcasing the range of methods available for extracting data efficiently and effectively in digital crime investigations [21].

5. CHALLENGES AND FUTURE DIRECTIONS

As the field of mobile forensics continues to evolve, it faces a myriad of challenges and opportunities for future growth and development. One of the primary challenges is the constant evolution of mobile devices, operating systems, and encryption technologies, which can make it difficult for forensic tools to keep pace. Additionally, the sheer volume and diversity of mobile devices in use present a daunting task for forensic investigators, who must stay up-to-date on the latest tools and techniques [21]. However, these challenges also present opportunities for further research and innovation in the field. Future directions for mobile forensics may involve the integration of artificial intelligence and machine learning algorithms to aid in data analysis and interpretation, as well as the development of specialized tools for emerging technologies such as IoT devices and drones. By addressing these challenges and embracing new technologies, the field of mobile forensics is poised for continued growth and success.

5.1. Legal implications and privacy concerns

The dynamic landscape of technological advancements in mobile platforms has ushered in a new era for digital crime investigation, presenting both opportunities and challenges. As smartphones become integral to everyday life, they also serve as potential tools for perpetrators to engage in criminal activities. The utilization of mobile forensics tools is paramount in extracting crucial digital evidence from Android devices to aid in criminal investigations. By comparing the performance of tools such as UltData Android, Wondershare Dr. Fone, and EaseUs Mobisaver, it is evident that the accuracy and efficiency of data restoration can significantly impact the outcome of legal proceedings. The ability to extract a wide array of data types, including contacts, messages, media files, and social media content, underscores the importance of employing advanced forensic techniques to ensure the integrity of digital evidence. In a world where information stored on mobile devices can make or break a case, continuous advancements in mobile forensics tools are imperative for staying ahead in the realm of digital crime investigation.

The use of forensic software tools for mobile devices raises important legal implications and privacy concerns that must be carefully considered. As these tools become more advanced and capable of extracting vast amounts of data from smartphones, cloud services, and IoT devices, the potential for privacy violations increases. The unauthorized access to personal information, communication records, and location data can infringe upon individual privacy rights and may even violate laws and regulations regarding data protection. In addition, the use of such tools for digital crime investigations must adhere to legal standards and procedures to ensure that any evidence obtained is admissible in court. Therefore, it is essential for forensic investigators to be aware of the legal implications of using these tools and to follow ethical guidelines to protect the privacy rights of individuals involved [21].

5.2. Rapid technological advancements

In the realm of digital forensics, rapid technological advancements have paved the way for sophisticated tools and techniques aimed at extracting and analyzing data from various mobile devices. The plethora of tools available, such as Cellebrite UFED, Oxygen Forensic Detective, and XRY by MSAB, each

offer unique functionalities and capabilities tailored to different use cases and scenarios, making them essential for digital crime investigations. These tools not only provide access to a wide range of devices, including smartphones, IoT devices, and drones but also offer different extraction methods such as physical and logical extraction, facilitated by connections like JTAG or Bluetooth (Mohammed Moreb, 2022). Moreover, with the continuous evolution of forensic software tools, new techniques such as chip-off and microread are being developed to further enhance the extraction process, showcasing the ongoing innovation in the field of mobile forensics.

5.3. Data encryption and security measures

Forensic software tools are constantly evolving to keep pace with advancements in technology and to address the challenges posed by data encryption and security measures. Encryption plays a crucial role in safeguarding sensitive information stored on mobile devices, making it essential for forensic investigators to have the means to decrypt this data effectively. Various techniques, such as physical and logical extraction, are used to acquire data from mobile devices, each with its own set of advantages and limitations. Additionally, tools like Cellebrite UFED, Oxygen Forensic Detective, and XRY by MSAB offer specialized capabilities for accessing and analyzing data from a wide range of mobile platforms. These tools enable forensic experts to effectively overcome encryption barriers and retrieve valuable evidence from a diverse array of devices, including smartphones, IoT devices, and drones. In essence, the continuous development and innovation in mobile forensics tools are instrumental in ensuring successful digital crime investigations by providing access to encrypted data and enhancing overall security measures [49].

5.4. Training and skill requirements for investigators

One crucial aspect of digital crime investigation is the training and skill requirements for investigators. To effectively utilize the diverse range of forensic tools available for mobile device analysis, investigators must undergo specialized training to enhance their technical proficiency and analytical skills. This training often covers various aspects such as data acquisition methods, evidence preservation techniques, data recovery processes, and legal considerations surrounding digital evidence. According to, investigators should possess a deep understanding of the different tools and techniques available for mobile forensic analysis to ensure accurate and thorough investigation outcomes. Additionally, Bair [50] emphasizes the importance of continuous professional development to keep abreast of the latest advancements in forensic technology and methodologies. By investing in training and skill development, investigators can enhance their capabilities to handle complex digital crime cases effectively and ethically.

5.5. Integration with other forensic tools

Forensic software tools are constantly evolving to enhance their capabilities for digital crime investigations. Integration with other forensic tools is vital for comprehensive analysis. By seamlessly incorporating data from different sources, investigators can paint a more complete picture of the case at hand. This integration allows for cross-referencing of evidence, ensuring accuracy and reliability in the investigative process. For example, integrating mobile forensics tools with network forensics tools can provide a deeper insight into communication patterns and network activities related to the case. Additionally, integrating tools that specialize in different aspects of digital forensics, such as malware analysis or data recovery, can further enrich the investigative process. The symbiotic relationship between various forensic tools enhances the efficiency and effectiveness of digital crime investigations. Through this collaborative approach, investigators can uncover critical evidence and build a strong case against perpetrators [18].

5.6. Standardization of procedures and protocols

One critical aspect in the realm of mobile forensics is the standardization of procedures and protocols. Ensuring that forensic tools follow standardized procedures is essential for the reliability and validity of investigative processes. Different tools often have varying methods of data acquisition and analysis, leading to potential inconsistencies in the results obtained. By establishing standardized protocols and procedures, such as those outlined by organizations like NIST, tools can be more effectively compared and evaluated for their efficiency and accuracy in digital crime investigations. Additionally, standardized procedures enhance interoperability among different tools, enabling smoother collaboration and data sharing among forensic examiners. This standardized approach ultimately strengthens the overall quality and effectiveness of mobile forensic investigations. Furthermore, it establishes a solid foundation for the field to continue advancing and adapting to the evolving landscape of digital crimes [22].

5.7. Emerging trends in mobile forensics

Mobile forensics has seen significant advancements in recent years, with a plethora of tools available for acquiring and analyzing evidence from various platforms. The landscape of mobile forensics tools includes

Mobile forensics tools and techniques for digital crime investigation: a comprehensive review (Tole Sutikno)

a wide array of options, such as Cellebrite UFED, Oxygen Forensic Detective, XRY by MSAB, and many more. These tools offer distinct features and functionalities, catering to different use cases and scenarios. They enable investigators to access and analyze critical data from a diverse range of devices, including smartphones, IoT devices, and drones. In the realm of data extraction techniques, physical and logical extraction methods stand out as the most commonly employed approaches [18]. Physical extraction involves JTAG or cable connections, while logical extraction relies on Bluetooth, infrared, or cable connections. Additionally, tools are classified based on their extraction methods, including manual extraction, hex dump, chip-off, and microread techniques. This ongoing evolution in mobile forensics tools underscores the importance of staying abreast of emerging trends in this dynamic field.

6. CONCLUSION

Mobile forensics is a crucial tool in the investigation of digital crime on Android mobile devices. It involves the use of various techniques and tools, such as Cellebrite UFED and Oxygen Forensic Detective, to identify, secure, and analyze digital evidence related to financial fraud and network crimes. These tools help investigators navigate the complexities of data acquisition, decryption, and analysis, reducing financial fraud risks and identifying perpetrators in network crime cases effectively. The interplay between mobile forensics and network forensics provides a holistic approach to digital crime investigations, emphasizing the need for sophisticated tools and methodologies. Notable tools include Cellebrite UFED, Oxygen Forensic Detective, XRY by MSAB, and Magnet AXIOM. These tools offer a wide range of features and functionalities tailored to different use cases and scenarios, allowing for data extraction and analysis from various mobile devices. The evolution of forensic software tools has led to the development of physical and logical extraction methods, with categories including manual extraction, logical extraction, hex dump, chip-off, and microread. In conclusion, the comparison of Android mobile forensics tools and techniques for digital crime investigation reveals a diverse landscape of tools with varying capabilities and approaches. Forensic tools provide comprehensive solutions for acquiring and analyzing evidence from mobile devices. However, there is a need for continuous development in this field as new data storage technologies and encryption methods present challenges for investigators. Future research should focus on the advancement of tools to keep pace with the evolving mobile technology landscape, ensuring effective investigation of digital crimes. Future research in Android mobile forensics tools and techniques for digital crime investigation should focus on the evolution of forensic software tools to keep pace with the ever-changing landscape of mobile technology. Advanced techniques for both physical and logical extractions are needed for accurate and thorough data recovery. Furthermore, a comprehensive classification system for forensic tools could streamline the investigation process by categorizing tools based on their extraction methods, simplifying the tool selection process for investigators. By addressing these future research areas, the field of mobile forensics can continue to advance and enhance its capabilities for digital crime investigation.

REFERENCES




- [1] I. Riadi, R. Umar, and A. Firdonsyah, "Forensic tools performance analysis on android-based blackberry messenger using NIST measurements," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 8, no. 5, pp. 3991–4003, 2018, doi: 10.11591/ijece.v8i5.pp3991-4003.
- [2] L. M. Jgaveerapandian, A. J. Rani, P. Periyaswamy, and S. Velusamy, "A survey on passive digital video forgery detection techniques," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 13, no. 6, pp. 6324–6334, 2023, doi: 10.11591/ijece.v13i6.pp6324-6334.
- [3] M. Hassan *et al.*, "Sentiment analysis on Bangla conversation using machine learning approach," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 12, no. 5, pp. 5562–5572, 2022, doi: 10.11591/ijece.v12i5.pp5562-5572.
- [4] R. Ruuhwan, I. Riadi, and Y. Prayudi, "Evaluation of integrated digital forensics investigation framework for the investigation of smartphones using soft system methodology," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 7, no. 5, pp. 2806–2817, 2017, doi: 10.11591/ijece.v7i5.pp2806-2817.
- [5] K. S. Vaddi, D. Kamble, R. Vaingankar, T. Khatri, and P. Bhalerao, "Enhancements in the world of digital forensics," *IAES International Journal of Artificial Intelligence (IJ-AI)*, vol. 13, no. 1, pp. 680–686, 2024, doi: 10.11591/ijai.v13.i1.pp680-686.
- [6] H. Tara and A. Mishra, "A comparative study of digital forensic tools for data extraction from electronic devices," *Journal of Punjab Academy of Forensic Medicine and Toxicology*, vol. 21, no. 1, pp. 97–104, 2021, doi: 10.5958/0974-083X.2021.00016.9.
- [7] P. Jain and A. Mishra, "Extraction of Data Using Cellebrite Ufed 4Pc," *International Journal of Medical Toxicology and Legal Medicine*, vol. 26, no. 3–4, pp. 222–232, 2023, doi: 10.5958/0974-4614.2023.00074.8.
- [8] F. Alshameri, K. Khanta, and S. Boyce, "A comparison study to analyse the data acquisitions of iOS and android smartphones using multiple forensic tools," *International Journal of Electronic Security and Digital Forensics*, vol. 16, no. 3, pp. 267–283, 2024, doi: 10.1504/IJESDF.2024.138325.
- [9] Á. Vizoso, M. Vaz-álvarez, and X. López-García, "Fighting deepfakes: media and internet giants' converging and diverging strategies against hi-tech misinformation," *Media and Communication*, vol. 9, no. 1, pp. 291–300, 2021, doi: 10.17645/MAC.V9I1.3494.

- [10] A. Zhang, B. Bradford, R. M. Morgan, and S. Nakhaezadeh, "Investigating the uses of mobile phone evidence in China criminal proceedings," *Science and Justice*, vol. 62, no. 3, pp. 385–398, 2022, doi: 10.1016/j.scijus.2022.03.011.
- [11] M. Michel, D. Pawlaszczyk, and R. Zimmermann, "AutoPoD-mobile-semi-automated data population using case-like scenarios for training and validation in mobile forensics," *Forensic Sciences*, vol. 2, no. 2, pp. 302–320, 2022, doi: 10.3390/forensicsci2020023.
- [12] N. Soni, M. Kaur, and V. Bhardwaj, "A forensic analysis of anydesk remote access application by using various forensic tools and techniques," *Forensic Science International: Digital Investigation*, vol. 48, 2024, doi: 10.1016/j.fsidi.2024.301695.
- [13] E. Daraghmi, Z. Qaroush, M. Hamdi, and O. Cheikhrouhou, "Forensic operations for recognizing SQLite content (FORC): an automated forensic tool for efficient SQLite evidence extraction on android devices," *Applied Sciences (Switzerland)*, vol. 13, no. 19, 2023, doi: 10.3390/app131910736.
- [14] J. Sablatura and U. Karabiyik, "Pokémon GO forensics: an android application analysis," *Information (Switzerland)*, vol. 8, no. 3, 2017, doi: 10.3390/info8030071.
- [15] I. Riadi, Herman, and N. H. Siregar, "Mobile forensic analysis of signal messenger application on android using digital forensic research workshop (DFRWS) framework," *Ingenierie des Systemes d'Information*, vol. 27, no. 6, pp. 903–913, 2022, doi: 10.18280/ISI.270606.
- [16] Y. Shin, S. Kim, W. Jo, and T. Shon, "Digital forensic case studies for in-vehicle infotainment systems using android auto and apple CarPlay," *Sensors*, vol. 22, no. 19, 2022, doi: 10.3390/s22197196.
- [17] M. Stanković, M. M. Mirza, and U. Karabiyik, "UAV forensics: DJI mini 2 case study," *Drones*, vol. 5, no. 2, 2021, doi: 10.3390/drones5020049.
- [18] O. Skulkin, D. Tindall, and R. Tamma, *Learning android forensics: analyze android devices with the latest forensic tools and techniques, 2nd Edition*. Packt Publishing, 2018.
- [19] A. Vasilaras, D. Dosis, M. Kotsis, and P. Rizomiliotis, "Retrieving deleted records from Telegram," *Forensic Science International: Digital Investigation*, vol. 43, 2022, doi: 10.1016/j.fsidi.2022.301447.
- [20] C. Serhal and N. A. Le-Khac, "Machine learning based approach to analyze file meta data for smart phone file triage," *Forensic Science International: Digital Investigation*, vol. 37, 2021, doi: 10.1016/j.fsidi.2021.301194.
- [21] A. Hoog, *Android Forensics: Investigation, Analysis and Mobile Security for Google Android*. Elsevier, 2011.
- [22] Tahiri Soufiane, *Mastering Mobile Forensics - Soufiane Tahiri - Google Książki*. Packt Publishing, 2016.
- [23] H. Bowling, K. Seigfried-Spellar, U. Karabiyik, and M. Rogers, "We are meeting on Microsoft Teams: Forensic analysis in Windows, Android, and iOS operating systems," *Journal of Forensic Sciences*, vol. 68, no. 2, pp. 434–460, 2023, doi: 10.1111/1556-4029.15208.
- [24] Y. Keim, S. Hutchinson, A. Shrivastava, and U. Karabiyik, "Forensic analysis of TikTok alternatives on Android and iOS devices: byte, dubsmash, and triller," *Electronics (Switzerland)*, vol. 11, no. 18, 2022, doi: 10.3390/electronics11182972.
- [25] H. Arshad, A. Bin Jantan, and O. I. Abiodun, "Digital forensics: Review of issues in scientific validation of digital evidence," *Journal of Information Processing Systems*, vol. 14, no. 2, pp. 346–376, 2018, doi: 10.3745/JIPS.03.0095.
- [26] I. Riadi, A. Yudhana, and G. P. I. Fanani, "Mobile forensic tools for digital crime investigation: comparison and evaluation," *International Journal of Safety and Security Engineering*, vol. 13, no. 1, pp. 11–19, Feb. 2023, doi: 10.18280/ijss.130102.
- [27] D. Kamble, S. Rathod, M. Bhelände, A. Shah, and P. Sapkal, "Correlating forensic data for enhanced network crime investigations: Techniques for packet sniffing, network forensics, and attack detection," *Journal of Autonomous Intelligence*, vol. 7, no. 4, Feb. 2024, doi: 10.32629/jai.v7i4.1272.
- [28] M. Okmi, L. Y. Por, T. F. Ang, W. Al-Hussein, and C. S. Ku, "A systematic review of mobile phone data in crime applications: a coherent taxonomy based on data types and analysis perspectives, challenges, and future research directions," *Sensors*, vol. 23, no. 9, p. 4350, Apr. 2023, doi: 10.3390/s23094350.
- [29] A. K. Mishra, M. C. Govil, E. S. Pilli, and A. Bijalwan, "Digital forensic investigation of healthcare data in cloud computing environment," *Journal of Healthcare Engineering*, vol. 2022, 2022, doi: 10.1155/2022/9709101.
- [30] M. F. Hyder, S. Arshad, and T. Fatima, "Toward social media forensics through development of iOS analyzers for evidence collection and analysis," *Concurrency and Computation: Practice and Experience*, vol. 36, no. 13, 2024, doi: 10.1002/cpe.8074.
- [31] J. Yang, J. Kim, J. Bang, S. Lee, and J. Park, "CATCH: cloud data acquisition through comprehensive and hybrid approaches," *Forensic Science International: Digital Investigation*, vol. 43, 2022, doi: 10.1016/j.fsidi.2022.301442.
- [32] I. Almomani, T. Almashat, and W. El-Shafai, "Maloid-DS: labeled dataset for android malware forensics," *IEEE Access*, p. 1, 2024, doi: 10.1109/ACCESS.2024.3400211.
- [33] P. Domingues, R. Nogueira, J. C. Francisco, and M. Frade, "Analyzing tiktok from a digital forensics perspective," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 12, no. 3, pp. 87–115, 2021, doi: 10.22667/JOWUA.2021.09.30.087.
- [34] P. Domingues, J. Francisco, and M. Frade, "Post-mortem digital forensics analysis of the zapp life android application," *Forensic Science International: Digital Investigation*, vol. 45, 2023, doi: 10.1016/j.fsidi.2023.301555.
- [35] E. Dragonas, C. Lambrinouidakis, and M. Kotsis, "IoT forensics: analysis of a HIKVISION's mobile app," *Forensic Science International: Digital Investigation*, vol. 45, 2023, doi: 10.1016/j.fsidi.2023.301560.
- [36] M. A. Mubarik, Z. Wang, Y. Nam, S. Kadry, and M. A. Waqar, "Instagram mobile application digital forensics," *Computer Systems Science and Engineering*, vol. 37, no. 2, pp. 169–186, 2021, doi: 10.32604/csse.2021.014472.
- [37] P. Domingues, L. M. Andrade, and M. Frade, "Microsoft's your phone environment from a digital forensic perspective," *Forensic Science International: Digital Investigation*, vol. 38, 2021, doi: 10.1016/j.fsidi.2021.301177.
- [38] L. Dawson and A. Akinbi, "Challenges and opportunities for wearable IoT forensics: TomTom Spark 3 as a case study," *Forensic Science International: Reports*, vol. 3, 2021, doi: 10.1016/j.fsir.2021.100198.
- [39] M. Negrão and P. Domingues, "SpeechToText: an open-source software for automatic detection and transcription of voice recordings in digital forensics," *Forensic Science International: Digital Investigation*, vol. 38, 2021, doi: 10.1016/j.fsidi.2021.301223.
- [40] S. A. Hashmi, "Malware detection and classification on different dataset by hybridization of CNN and machine learning," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 12, no. 6s, pp. 650–667, 2024.
- [41] T. Groß, M. Busch, and T. Müller, "One key to rule them all: recovering the master key from RAM to break Android's file-based encryption," *Forensic Science International: Digital Investigation*, vol. 36, 2021, doi: 10.1016/j.fsidi.2021.301113.
- [42] M. Surya, J. Sidabutar, and N. Qomariasih, "Comparative analysis of recovery tools for digital forensic evidence using NIST framework 800-101 R1," in *Proceedings - 2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity: Cryptography and Cybersecurity: Roles, Prospects, and Challenges, ICOCICs 2023*, Aug. 2023, pp. 258–262, doi: 10.1109/ICOCICs58778.2023.10276447.

- [43] H. H. B. Bhushan and S. M. Florance, "An overview on handling anti forensic issues in android devices using forensic automator tool," in *SPICES 2022 - IEEE International Conference on Signal Processing, Informatics, Communication and Energy Systems*, Mar. 2022, pp. 425–430, doi: 10.1109/SPICES52834.2022.9774183.
- [44] J. R. Hildebrandt, E. M. Schomakers, M. Ziefle, and A. C. Valdez, "Understanding indirect users' privacy concerns in mobile forensics — A mixed method conjoint approach," *Frontiers in Computer Science*, vol. 5, 2023, doi: 10.3389/fcomp.2023.972186.
- [45] L. Reiber, *Mobile forensic investigations : a guide to evidence collection, analysis, and presentation / Lee Reiber*. McGraw Hill LLC, 2019.
- [46] M. Moreb, *Practical forensic analysis of artifacts on iOS and Android devices*. Berkeley, CA: Apress, 2022.
- [47] A. Rocha and T. Guarda, *Proceedings of the International Conference on Information Technology & Systems (ICITS 2018)*, vol. 721. Cham: Springer International Publishing, 2022.
- [48] H. Dubey, S. Bhatt, and L. Negi, "Digital forensics techniques and trends: a review," *International Arab Journal of Information Technology*, vol. 20, no. 4, pp. 644–654, 2023, doi: 10.34028/iajit/20/4/11.
- [49] A. Harisha, A. Mishra, and C. Singh, *Advancements in cybercrime investigation and digital forensics*. Boca Raton: Apple Academic Press, 2023.
- [50] J. Bair, *Seeking the truth from mobile evidence: basic fundamentals, intermediate and advanced overview of current mobile forensic investigations*. Elsevier, 2017.

BIOGRAPHIES OF AUTHORS



Tole Sutikno    is a lecturer and the head of the Master Program of Electrical Engineering at the Faculty of Industrial Technology at Universitas Ahmad Dahlan (UAD) in Yogyakarta, Indonesia. He received his Bachelor of Engineering from Universitas Diponegoro in 1999, Master of Engineering from Universitas Gadjah Mada in 2004, and Doctor of Philosophy in Electrical Engineering from Universiti Teknologi Malaysia in 2016. All three degrees are in electrical engineering. He has been a Professor at UAD in Yogyakarta, Indonesia, since July 2023, following his tenure as an Associate Professor in June 2008. He is the Editor-in-Chief of TELKOMNIKA and Head of the Embedded Systems and Power Electronics Research Group (ESPERG). He is one of the top 2% of researchers worldwide, according to Stanford University and Elsevier BV's list of the most influential scientists from 2021 to the present. His research interests cover digital design, industrial applications, industrial electronics, industrial informatics, power electronics, motor drives, renewable energy, FPGA applications, embedded systems, artificial intelligence, intelligent control, digital libraries, and information technology. He can be contacted at email: tole@te.uad.ac.id.