Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 235 (2024) 1332–1352

Procedia Computer Science

www.elsevier.com/locate/procedia

International Conference on Machine Learning and Data Engineering (ICMLDE 2023)

A Systematic Literature Review on Digital Forensic Investigation on Android Devices

Almaha Almuqren[a] , Hanan Alsuwaelim[a] , M M Hafizur Rahman [a], Adamu A. Ibrahim[b] *

[a] *Department of Computer Networks and Communications King Faisal University, Saudi Arabia*
[b] *Department of Computer Science, KICT, International Islamic University, Malaysia (IIUM), Kuala Lumpur, Malaysia.*

Abstract

Mobile forensics, particularly in the Android ecosystem, is a rapidly evolving field that demands continuous advancements to address the growing complexity and diversity of mobile devices. This article emphasizes the importance of developing techniques for digitally analyzing Android smartphones, which dominate the smartphone market. The primary objective of this research is to contribute to the development of effective forensic investigation strategies tailored specifically for Android mobile devices, providing insights into the tools and methods used for this purpose. The objective of this study is to improve the precision and effectiveness of forensic examinations pertaining to Android mobile phones. It discusses the fundamental functionality of mobile devices as a source of digital evidence and provides an overview of tools and methodologies for collecting and analyzing such evidence. The importance of comprehending the hardware and software architecture of Android handsets in order to choose the right forensic tools is also highlighted in the article. Furthermore, it proposes future enhancements for Andriller, a popular digital forensic tool, to improve its effectiveness in Android forensic investigations. These enhancements include advancements in data extraction techniques, compatibility with new Android versions, support for additional data types, integration with advanced analysis methods, and addressing identified limitations. Additionally, the paper stresses the need for robust methodologies for conducting cloud forensics on Android devices, particularly in the context of data stored in cloud storage services. The proposed work aims to enhance the capabilities of Andriller and improve the efficiency of digital forensic investigations on Android devices.

* Corresponding author. Tel.: +966569009994; fax: +0-000-000-0000 .
E-mail address: 222400079@student.kfu.edu.sa

1877-0509
10.1016/j.procs.2024.04.126

Peer-review under responsibility of the scientific committee of the International Conference on Machine Learning and Data Engineering

Keywords: Forensic; Mobile devices ; Mobile Forensic ; Mobile Device Forensics; Andriller ;

1. Introduction

There is a great need for digital forensic specialists to incorporate these technologies into daily life because information technology (IT) systems and smart devices such as computers, smartphones, smartwatches, and other Internet of Thing's devices are becoming more and more common. Furthermore, the amount of data to be analyzed has increased to the point where manual digital forensic analysis is frequently impractical. This is a result of the abundance of data available now. To handle the enormous volume of data, software and hardware forensic tools that automate some or maybe all of the processing is required. These instruments may be hardware based or software based. In addition, the wide range of device types, each of which can be constructed uniquely and runs a different operating system, makes it difficult to employ the digital forensic tools that are available [3].

It is common practice to divide digital forensics into five primary groups. Database forensics, network forensics, mobile forensics, and forensic data analysis are the four sub-fields that make up forensics. Each subfield of digital forensics brings something unique to the table when it comes to tracking down hackers, fraudsters, and phishers. The field of mobile forensics is one that is constantly evolving and needs to keep up with the advancements achieved in the field of information technology more generally. Because of the significant shifts in operating systems that can take place in a relatively short amount of time, the procedures and procedures that mobile forensics experts need to use in order to obtain and examine the data on a smartphone may need to be modified. This is the case even though mobile forensics experts are required to use them. The introduction of the first gadget that would later be called a smartphone was one of the biggest turning events in the history of the mobile phone industry. Unlike conventional mobile phones, smartphones are equipped with an extensive operating system and numerous additional applications that enable users to engage with an extensive range of voice and data services. The massive amounts of data that can be stored in processors as small as mobile phones is mind boggling. This study is summarized in Fig. 1. from the mobile phone forensic perspective.

Fig. 1. Overview of mobile phone forensics.

The method of taking digital evidence out of mobile devices in accordance with predefined protocols is known as mobile forensics. Mobile forensics, in contrast to more traditional techniques used in digital forensics, is primarily concerned with the process of extracting data from mobile devices such as smartphones, Androids, and tablets. Mobile devices save a plethora of information, including text messages, a history of online searches, and location data, all of which might be helpful to law enforcement investigations if the devices are seized. Whether it be file based encryption, full disk encryption, or hardware that is password protected, various software applications and operating systems make use of a variety of encryption techniques. When faced with a challenge of such nature, we have little choice but to look into other ways to acquire that knowledge. Android continues to be the most popular mobile phone operating

system globally. Presently, it is quite common to own an Android phone. Every digital forensics specialist must be able to do forensic testing on an Android phone. In this article on digital forensics, we are going to focus on Andriller [36]. Android devices have become a ubiquitous part of modern life, with millions of users relying on them for communication, entertainment, and productivity. However, the widespread use of these devices has also led to an increase in criminal activity involving them, such as cyberbullying, hacking, and theft. As a result, digital forensic investigation on Android devices has become an important area of study for law enforcement agencies and forensic investigators. This paper will provide an overview of digital forensic investigation on Android devices, including the tools and techniques used, and the challenges and limitations of this type of investigation [37].Andriller is a set of forensic tools for cellphones included within a software application. It acquires data from Android devices in a nondestructive, read only manner that is forensically sound. We will install Andriller on our kali Linux system and do testing on our own device. The following are this paper's primary contributions:

- Examine and compare various forensic tools and techniques for Android mobile devices.
- We compare physical, logical, and manual data acquisition methods in Android mobile forensics.
- Determine security and privacy vulnerabilities on an Android device.
- Provide the first comprehensive forensic analysis of an Andriller on Android.
- The Android forensic investigation is one of the most significant contributions to the body of knowledge. Forensic Analysis of an Android Phone After backing up your Android phone using Andriller, choose any of the options, such as WiFi password, to retrieve all the information stored in this folder.

This paper's remaining sections are organized as follows: (1) Examine the tools or methods suggested for mobile forensics; (2) Using a mobile phone as evidence; (3) Obstacles Faced by Mobile Forensics; (4) Android Device Forensics; and (5) Other Issues Concerning Android Forensics. The review concentrates its attention, for the most part, on English literature that was accessible through public data sources between the years 2019 and 2023. This study's primary objective is to investigate fundamental forensic problems about the recoverability of cached material and metadata for streaming services running on the Android operating system.

2. Scope

The widespread use of mobile technology is perhaps the primary cause of this paper, or at least one of the primary causes. The Internet of Things, big data, and cloud computing are three emerging technical advancements that are directly influencing mobile devices. Today, the usage of mobile devices is widespread and advantageous, particularly in the field of digital forensics, because these compact devices gather massive amounts of data on a regular basis that may be recovered to aid the investigation. These devices give digital forensic investigators access to a wealth of information since they act as a kind of digital extension of ourselves. These days, mobile devices are widely used and beneficial, especially in the field of digital forensics, where these small devices regularly collect large amounts of data that might be recovered to strengthen the case. Given that these gadgets function as a sort of digital extension of ourselves, digital forensic investigators have access to an abundance of data.

3. Motivation

The forensic investigation must begin with mobile device identification. To generate a legitimate copy of the mobile device's material, the identification procedure includes knowledge of the type of cell phone, its OS, and other crucial aspects. Mobile forensics offers a wide range of tools and methods. However, the kind of mobile device and the media it is connected to determine the tools and methods used during an investigation.

4. Mobile Devices

There are numerous mobile devices. Smart phones have arguably, evolved into a need in our society over the past ten years, becoming more than just a staple. Mobiles are used for a variety of communications, including making phone calls, sending text messages, sending emails, and interacting with friends and family through various social network-ing or instant messaging services. There are several mobile device types and subcategories, including PDAs, portable devices, eBook readers, and smart phones. In the smartphone industry, Android and Apple are the two main

competitors. The market for smartphones is dominated by Android devices, with Apple coming in second. Other smartphones do exist, such as Windows OS and Blackberry models, but their share of the overall smartphone market is incredibly small. Smartphones powered by Android are portable hybrid devices capable of performing the functions of a mobile phone and a computer. In light of the significance of the data saved on these mobile phones, research in the field of mobile device forensics has gained steam.

4.1. Mobile Forensic

The most obvious instances of digital evidence are computers and the hard drives, floppy disks, and optical disks that go along with them. Numerous devices, such as personal digital assistants, music players, cameras, watches, GPS units, mobile phones, fax machines, and security access devices, can include digital evidence embedded in them or connected to them. Many modern credit cards include an incorporated computer chip; for this reason, they are frequently called "smart cards." New devices are developed almost daily, and as time goes on, electronics get faster and have larger storage capacities. Data that is not static is the only reliable source of information. Data communications via cables and wireless links can both be intercepted. In the dynamic domain, packetized signals are transmitted over analogous physical media, including radio frequency carriers, infrared, and coaxial and braided cables.

The study of recovering digital evidence from a mobile phone using forensically sound configurations and authorized procedures is known as mobile phone forensics. Numerous studies have been conducted on the topic of mobile forensics; some focus on Android and iPhone forensics, while others address mobile forensics in general. There are many techniques to carry out forensics on GSM phones, however Android forensics is the main focus of this essay. Mobile phones use flash memory to store data. Flash memory has the advantage of being more resistant to damage because it can withstand impact, extreme temperatures, and pressure. From a forensic perspective, this is helpful because they might still have deleted data even if the individual tries to remove the proof.

4.1.1. Types of Evidences

Digital evidence is stored or transferred information with evidence with a binary value format. This definition states that, There is more evidence than that discovered evidence from digital devices like telecommunication or electronic multimedia devices, but it could also involve evidence from computers. In addition, Electronic proof is not restricted to classic hacking and other cybercrimes infiltration but encompasses all criminal categories where digital evidence may be discovered. Due to the nature of digital evidence, its admission in court presents unique obstacles. The procedure includes four independent but interdependent steps: collection, inspection, analysis, and reporting. Typically, warrants for searches of electronic storage devices concentrate on two key information sources:

1. Warrant for the search of electronic storage devices.
    - examination and confiscation of storage media, user notes, documentation, gear, and software
    - Inspection, tracking, and acquisition of data
2. Warrant search for a service provider
    - Service and billing documents, as well as subscriber documents.
    - Request details provided by service providers, including utilities, banking institutions, telephone companies, and cable companies.

4.1.2. Mobile Phone as Evidence

Mobile device forensics, the information acquired from mobile phones is probative. These pieces of evidence are crucial when law enforcement authorities conduct an investigation. Several types of evidence may be gathered from mobile devices. The evidence that may be retrieved from a mobile phone includes contacts, call records, test messages, audio recordings, email, and internet activity. These objects may be retrieved logically or physically. Logical extracts data from the file system by communicating directly with the device using specialized software. The SIM (Subscriber Identity Module) is a crucial component of mobile phones. This little chip put into the mobile phone provides extra storage space for data. For the goal of extracting data from SIM, there exist specialized tools such as SIMbrush [11]. Not only may information storage differ from device to device and operating system to operating system, but devices

may also be passcode- or encryption-protected. Obviously, it is simple to retrieve information from a smartphone without a passcode.

A mobile data extraction program should be able to automatically generate a simple passcode for all devices. Following the extraction of the pass code, it will be possible to extract and rewrite any data, even protected files. Android devices may even be locked by the user. Once decoded, a classification system or physical extraction might provide the correct pattern or PIN code to lock the device. Alternatively, if decryption is not enabled by the extraction tool, the PIN lock should be able to be hacked. This is due to the fact that hardware and chipsets vary between devices, affecting the degree to which a rhetorical tool can replicate the classification scheme. From a forensic perspective, mobile devices provide a big advantage though: even if the user has attempted to destroy the data, it can still be there on the device. The main reason why deleted data remains on mobile devices is that Flash memory chips are used to store data. Because flash memory is physically resistant to pressure, high temperatures, and other environmental stresses, it is more difficult to destroy. Additionally, mobile devices usually wait until a block is full before deleting data from flash memory since it can only be erased block-by-block and has a limited write capacity. Additionally, mobile devices disperse write and erase operations among Flash memory blocks using proprietary wear leveling algorithms. This might cause erased data to stay in memory for a long time while fresh data is written to less frequently visited memory locations. It is necessary to obtain a whole copy of physical memory in order to recover and restore earlier or erased versions of data [36].

Table 1. The location of mobile evidence.

Mobile Evidence	Location
Service provider	On the back of SIM
Unique Identity Number	On the back of SIM
Location Area Identity (LIM)	Saved Inside the SIM
Call logs	Stored on both SIM and phone memory
Contacts	Stored on both SIM and phone memory
International Mobile Subscriber Identity (IMSI)	is unique to each subscriber and stored inside the SIM
Text message data	Stored inside the SIM and phone memory
Multimedia messages	Stored on phone memory
Images/videos/sound	Stored on phone memory
Calendar	Stored on phone memory
WAP/Browser history/Emails	Stored on phone memory
Previous SIM data	Not all phones stores the previous SIM data
Telephone number	Sometimes present in SIM memory
Integrated Circuit Card Identifier (ICCID)	Stored inside SIM
International Mobile Equipment Identity (IMEI)	Stored and printed on mobile phone

4.2. Ethical Guidelines for Digital Forensic Investigators

Digital forensic investigators collect and analyze digital evidence to support legal proceedings. As such, they must follow ethical guidelines to ensure that their investigations are conducted fairly and impartially and that the individuals' rights are protected. Here are some standard ethical guidelines that digital forensic investigators must follow:

- Respect for individual rights: Digital forensic investigators must respect the legal and constitutional rights of the individuals involved and ensure that their investigation does not infringe on their privacy or other legal rights. Investigators must obtain legal permissions and warrants before accessing digital devices or data.
- Objectivity: Digital forensic investigators must be objective and impartial in their investigations. Any biases or preconceived notions can lead to inaccuracies while examining digital data and are capable of result in the misinterpretation of findings.
- Confidentiality: Digital forensic investigators must maintain confidentiality and ensure that any sensitive information obtained during the investigation is protected and not disclosed to unauthorized individuals. The digital evidence collected must be secured and protected from unauthorized access.
- Integrity: Digital forensic investigators must maintain the reliability of the gathered digital evidence during the investigation and ensure that it is not tampered with or altered. Investigators must follow recognized best practices in digital evidence collection and analysis to guarantee the admissibility of the evidence in court.

- Professionalism: Digital forensic investigators must conduct themselves professionally and adhere to the highest standards of ethical conduct. Investigators must maintain a high level of competence in their field and keep up with the latest developments in digital forensics.
- Compliance with legal and regulatory requirements: Digital forensic investigators must comply with all legal and regulatory requirements applicable to their investigation. Investigators must follow the applicable laws and regulations and obtain legal permissions and warrants before conducting any investigation.

By following these ethical guidelines, digital forensic investigators can ensure that their investigations are conducted fairly and impartially and that the digital evidence collected is admissible in court.

5. Literature Review

This systematic literature review examines the current state of digital forensic investigation on Android devices. The review follows the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines and includes an analysis of recent publications. According to the PRISMA guidelines, one of the reasons for excluding records is their lack of relevance or inability to address the research question (the quantity of papers, reason 5). These documents are regarded as extraneous and, as such, are ineligible for inclusion in the review. Studies that do not satisfy the intended methodological criteria (number of papers, reason 4) are another cause for exclusion. This criterion enables researchers to exclude studies that do not meet the specific requirements for research design, ensuring that only studies that adhere to the intended methodology are included. In addition, the exclusion of studies published in excluded languages or publication categories that do not satisfy the review's criteria is documented (the number of papers, reason 1). More importantly, this practice ensures that the review concentrates on studies published in the specified languages and publication formats, thereby maintaining consistency and relevance throughout the selection process. The study provides an overview of the tools and techniques used in digital forensic investigation on Android devices, including the Andriller, as well as file carving, keyword searching, and timeline analysis. This literature review provides valuable insights for forensic investigators and researchers seeking to enhance their knowledge of digital forensic investigation on Android devices.

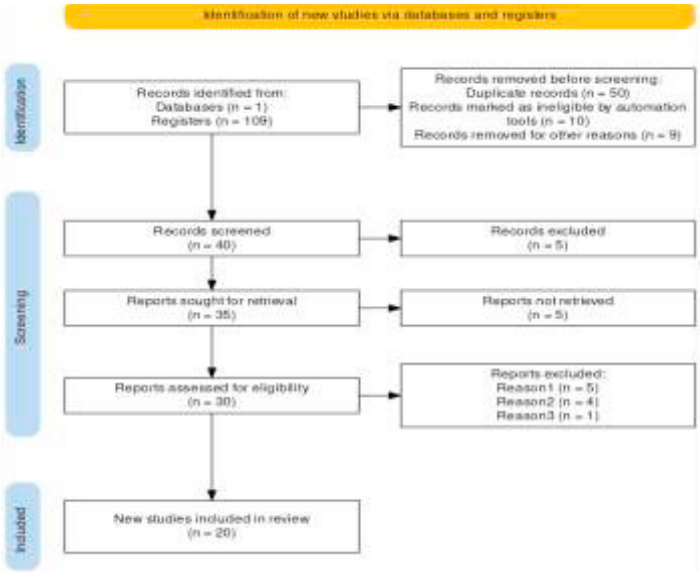


Fig. 2. Selection of papers by using PRISMA

5.1. Related Work

In this study, digital forensics were done on the Facebook Messenger program using data deletion and application uninstallation scenarios. The data, photos, and videos sent by the cybercriminal through the Facebook Messenger app serve as digital evidence of what was found [13]. In this paper, they analyze the efficacy of applying principle

component analysis to the computational forensics problem of identifying Android-based malware [14]. The method employs a hybrid study consisting of static program analysis of the Android Framework and forensic analysis of operating system images in order to identify access routes. With an F1 score of 91.348%, the new technique exceeds the prior baseline model [15]. This paper examines the crimes committed on social networking sites, as well as phishing, cyberbullying, link baiting, and digital evidence analysis. To retrieve digital evidence from mobile devices using forensic procedures, mobile device forensics and forensically sound approaches are used [16]. In this research, they devised and implemented a trustworthy detection approach based on memory comparison and the Joint Test Action Group (JTAG) that can accurately identify common firmware tampering threats. The findings of the trial demonstrate that Aye can successfully resist firmware tampering assaults, enhancing the effectiveness and precision of such attack detection and forensics [17].

The comparison of Apple CarPlay with Android Auto from this angle is inadequate. As a result, they suggested a forensic technique that completely takes into account these constraints. Several IVI systems were subjected to a forensic study. In addition, they created an IVI system forensics tool [18]. The objective of the study is to help scientists unleash the full potential of popular cryptocurrency wallets like Web3, Trust Wallet, and Metamask, as well as identify knowledge gaps. They digitally evaluated and forensically inspected two mobile wallets that do not need any personal information to register and are extensively used on Android and iOS smartphones for Web3 cryptocurrencies [19]. In this work, the likelihood of data recovery was measured by looking at the filesystem information before and after user data was deleted on devices that ran Android platforms 9 and 10[20]. This study examines the forensically significant artifacts that may be retrieved from the controlling software for the newly introduced Amazon Halo fitness band, as well as the TicWatch and Garmin fitness trackers on an Android smartphone device [21]. The Oppo F9 and Samsung S7 Edge, two Android-based smartphones, will be used in this research to explore, perform, and assess logical acquisition utilizing Wondershare Dr. Fone for Android, MOBILedit Forensic, and FonePaw for Android. The study is based on the efficiency and testing time for each mobile forensic tool on the two Android phones that were chosen [22].

The overall information, the structure of the Android, and the key artifacts are all presented in this paper. investigates various techniques for obtaining memories and artifacts from the device's internal and external memories, the difficulties these methodologies face, and how to analyze all of the aforementioned information in order for the investigator to find crucial evidence for the case and the device user [23]. This research begins by identifying prospective data and methods for creating custom datasets for Android mobile forensics. Second, it lays the groundwork for further investigation into the use of mobile forensic emulators for teaching [24]. In this paper, a technique for data extraction and forensic analysis of these data has been described by analyzing the structure of the Android-based Discord program [25]. Criminal and forensic investigators use the assistance of digital forensics while conducting investigations in order to determine whether or not the victim committed the crime they are looking into. This article provides a description of some recent advancements in digital forensics tools and examines new issues that are appearing in more sophisticated areas of digital forensics [26]. This study focuses on how antiforensic difficulties in android mobiles may be addressed and how advancements have been made in the fields of mobile forensics and data gathering [27].

The increasing prevalence of Android-powered smartphones renders them susceptible to cyberattacks. This article provides an overview of Android mobile device forensics [28]. This study provides an effective forensics investigation approach for mobile devices running the Android operating system, which boasts the largest market share of any mobile operating system in the world. In this article, they analyzed data pre-processing (data categorization and identification), data analysis, evidence management, and Android data taxonomy [29]. This research will demonstrate that most mobile forensics tools heavily depend on rooted (Android) smartphones to retrieve data. As some of the chosen studies in this study will demonstrate, rooting offers a significant difficulty for forensic analysts in maintaining the integrity of user data [30]. In this research, the authors undertake a study of mobile forensics investigation process models (MFIPMs) as a means of revealing MF transitions and highlighting open and future difficulties. A review of the literature indicated, based on the research presented in this article, that there are a number of MFIPMs created to solve specific mobile situations, including a range of ideas, inquiry processes, activities, and tasks [31]. This study collects digital evidence using the Universal Forensic Extraction Device (UFED) and MOBILedit tools. The social media platforms that forensic investigators will examine are Instagram, Line, WhatsApp, Facebook Messenger, Skype, Snapchat, Viber, and Telegram [32]. This article examines some of the technological concerns with the

Android WhatsApp application that might facilitate cybercrime and provide anti-forensic hurdles. In addition, they suggest a proven solution to the "delete for everyone" function of WhatsApp by showing a demonstration mobile application that retrieves any deleted messages even after a block status[33]. The author say Mobile Forensics can assist in supplying information, particularly by locating numerous alternatives or contacts who often engage with suspects. By obtaining the suspect's cell phone and utilizing the Oxygen Forensic and Andriller tools, I was able to locate a lot of papers that are suspicious and helpful in police work[35]. After reviewing the papers, each of these tools has advantages and disadvantages, and the decision will depend on a company's or individual's needs. but in this paper, we determined that the Andriller tool was one of the best, so it will be used in this paper. Table 2 lists the technologies and their potential uses for mobile forensics.

Table 2. The review for mobile forensics.

ref	Objective	Tools & Techniques	Data Acquisition
19	The objectives of this research are to fill information gaps, comprehend what may be retrieved, and unleash the potential of well-known Bitcoin Web3 wallets.	iLEAPP, the iOS Logs, Events, and Plists Parser	Data Acquisition: We ensured that we could gather user data with the appropriate instruments in addition to taking into account the distinctive features of the iOS and Android operating systems.
20	This study investigates the deleted data that is still there on the device and whether it can be recovered to enhance user privacy on Android 9 and 10. Three possibilities for data destruction are used.	The app's own function, the system app's data and cache deletion function, and the uninstallation of installed apps are the three data deletion procedures it employs.	-
18	A forensic technique for analyzing IVI systems has been presented, and a tool for IVI system forensics has been built based on this methodology.	The Charles Proxy tool is used to consume packets from cloud storage and mobile devices.	The built-in Wireshark and BT Snoop utilities on Android devices are utilized for acquisition and analysis. The PacketLogger and Wireshark tools in Xcode are used for iOS devices.
31	This paper examines Mobile Forensics Investigation Process Models (MFIPMs) in order to identify current and upcoming issues as well as the MF transitions. In order to streamline and organize duplicate investigative activities, it suggests using the Harmonized Mobile Forensic investigative Process Model (HMFIPM).	The authors take a step to evaluate Mobile Forensics Investigation Process Models (MFIPMs) in order to discover open and future difficulties and to expose the MF transitions.	The two sub-processes of the data acquisition process—live and dead—are utilized to gather both volatile and non-volatile data from a possible mobile device.
17	The detection of firmware-tampering assaults may be reliably detected using the methods they devised and implemented in this work, which is based on JTAG and memory comparison.	Two of the most recent PLC firmware manipulation attack methodologies were simulated in order to assess Aye's reliability in detecting popular firmware tampering attempts.	The identification and mapping of the memory content of a firmware tampering attack requires JTAG-based PLC memory content acquisition and mapping.
21	The authors conducted a forensic analysis of three popular fitness bands and smartwatches in order to report evidence relevant to forensics and highlight privacy concerns.	employed open source	

5.2. The importance of forensics for mobile phone handsets

The subsequent portion of the article will explain the necessity for mobile forensics by focusing on the following:

- The use of mobile devices to store and transfer data.
- Utilization of mobile devices for online transactions.
- Law enforcement, for criminals, and mobile phone technology.

5.2.1. The use of mobile devices to store and transfer data.

Mobile phones become portable offices thanks to their capacity to store, browse, and print electronic documents. Mobile devices became message centers when they gained the capacity to send and receive Short Message Service (SMS) messages. Additionally, innovations like "push e-mail" and always-on connectivity gave mobile devices additional convenience and potent communications capabilities [7]. The mobile phone was then able to store and transmit emails because of this. Approximately 80% of Internet users worldwide today have access to the Internet

while on the go. The most common online activities among mobile Internet users include web searching, viewing news and sports content, downloading music, movies, ringtones, utilizing instant messaging, and sending email over the internet.

5.2.2. Utilization of mobile devices for online transactions.

Mobile phones may now be used for online transactions due to the Wireless Application Protocol (WAP) [8]. The use of mobile phones for safe transactions like stock trading, online shopping, mobile banking, hotel bookings and check-in, and travel confirmations and reservations is made possible by further improvements in the connection and security of mobile devices and networks.

5.2.3. Law enforcement, for criminals, and mobile phone technology.

Concerning the use of mobile phone technology, the gap between law enforcement and organized crime remains substantial. In contrast, law enforcement and digital forensics continue to lag behind when it comes to processing digital evidence gathered from mobile devices [9]. This is attributable in part to the following factors:

- The device's mobility requires specific interfaces, storage media, and hardware.
- The file system is stored in volatile RAM rather than on independent hard disks.
- The large number of embedded operating systems in use today.
- The short time span between the release of new devices and the accompanying operating systems.

Because of these differences, it is important to know the difference between computer forensics and mobile phone forensics.

5.3. Security threats in mobile forensics

Maintaining a steady rate of change with mobile technologies is the largest issue for mobile forensics. Every day, new hardware and operating systems with distinct file systems and data storage strategies are released [4]. Experts in mobile forensics find it difficult to stay up to date with the most recent modifications as a result. The following categories more broadly describe the difficulties with mobile forensics:

- Device loss or theft

Due to the small size and portability of mobile devices, it is easy to misplace them. Lost gadgets may fall into the wrong hands, allowing unauthorized access to the device's data and information [9].

- Malware and other mobile device threats

Mobile devices, like all internet-connected gadgets, are vulnerable to malware, phishing, and other cyber assaults. This vulnerability grows when these devices use public Wi-Fi or unsecured networks to connect to the internet.

- Human mistake

Humans remain the weakest link when it comes to cybersecurity. Humans are renowned for clicking on erroneous links or falling for phishing emails, allowing cybercriminals to get unauthorized access to mobile devices.

Mobile forensics can assist in mitigating the hazards associated with lost or stolen mobile devices by enabling enterprises to remotely delete data from lost or stolen devices. Mobile forensics can also aid in the investigation of potential mobile security breaches and data recovery. Lastly, mobile forensics tools can be used to teach employees how to protect firm data on mobile devices in the best way possible [4].

5.4. Mobile Phone forensics' challenges

The largest issue in mobile forensics is keeping up with the rapid speed of change in mobile technologies. There is a steady release of new devices and operating systems, each with its own file system and data storage mechanisms. This makes it tough for mobile forensics experts to stay current with the latest improvements. In a broader sense, the challenges associated with mobile forensics can be categorized as follows [5,35,37]:

- Differences in hardware: There are a variety of hardware configurations for mobile devices of varying sizes and shapes. This makes it difficult to create mobile forensics tools that function on all devices [18].

- Password security and encryption: There is Several mobile devices are encrypted and password-protected, making data recovery and mobile forensics challenging.
- Lack of tools and equipment: Mobile forensics is still a very young field with limited available tools. This makes it challenging to conduct mobile forensics effectively.
- Dynamic nature of evidence: The continual evolution of mobile devices makes it tough to keep track of all the data on a device. A user may install a new application or delete an existing one, which can alter the device's data. This makes it difficult to distinguish between useful and irrelevant material [3].
- Anti-forensic techniques: As mobile forensics gains popularity, criminals are also becoming more aware of it and employing anti-forensic measures to prevent their data from being recovered.
- Legal issues: Mobile forensics can be used to recover a great deal of sensitive information that can be used in court. Nonetheless, numerous rules govern the use of this information. For example, there are laws that protect the privacy of users.
- Device alteration: Mobile devices are easily modifiable. A user may, for instance, root their device, which modifies the device's default data and makes it harder to recover.
- Mobile platform security features: Numerous mobile devices include security mechanisms that might make data retrieval challenging. For instance, Apple's iPhone contains a "Secure Enclave" feature that encrypts all of the device's data.
- Communication shielding: This is when a user uses a mobile device to communicate with a person with whom they do not wish to be monitored. For instance, they may utilize a disposable phone or texting software with encryption. This can make it more difficult to retrieve the data from the mobile device [26].
- Preventing data modification: Mobile forensics seeks to preserve the data on a mobile device so that it can be used as evidence in court. This can be challenging, though, if the data is continuously updated. Many mobile devices discard old data automatically to make place for fresh data. This can make recovering erased data challenging.
- Malicious programs: These programs are intended to prevent mobile forensics specialists from obtaining mobile device data. A user may install a program that encrypts all data on their device.
- Mobile operating systems: There are numerous mobile operating systems, each with its own file system and methods for storing data. This can make data collection and analysis more challenging.
- Accidental device reset: Accidental device resets are one of the most frequent challenges mobile forensics experts confront. This may wipe all of the device's data, making it difficult to restore.

5.5. Mobile forensics investigation of cybercrime

Cybercrime is the term used to describe crimes carried out using digital tools like computers and other networked devices. Cybercriminals illegally access another person's computer or networked device, which they then utilize for activities like money theft or holding data hostage for ransom. While tackling cybercrime, appropriate techniques for data collection are crucial. In addition, it can be difficult to successfully carry out a digital inquiry using a mobile device. There are numerous causes for this problem. For instance, it is impossible to produce a precise bitwise copy of the whole contents of the device's memory due to the continuous operation of the device clock on mobile devices. The short OS release cycle employed by various mobile phones presents another difficulty [32-35]. Because of this, the timely updating of forensic tools to reflect changes in operating systems is challenging. Typically, there are two parts to a cybercrime investigation:

To ensure the guilty party is brought to justice, the guilty party must be located and evidence must be gathered.

Ensuring that the person or company that was the victim of the theft is able to regain use of their tools and any money stolen.

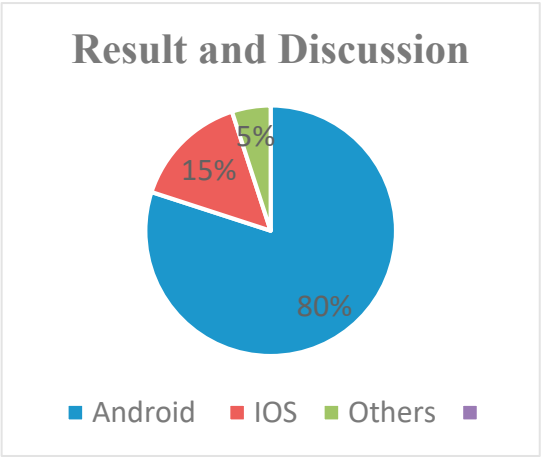
Digital forensic investigations must adhere to a specific method in order to protect data integrity and guarantee that guilty parties can be found guilty in court. Therefore, it is essential for every digital forensic researcher to have a thorough understanding of the best data collection techniques.

5.6. Result and Discussion

The collection of mobile devices, also a lot of the forensic tools are utilized. Mobile device data preservation differs significantly from computer data preservation and forensic hardware and software. There are several types of collections that can be conducted using mobile devices. The vacant space on mobile devices is preserved bit by bit in physical collections. Logical collections only store the user's data, not the phone's unused space. File system collections, which are similar to logical collections but may pull more information, keep only the file system. Manual collection would be the final option for mobile device collection. This is typically employed when a forensic tool cannot access a device due to age or operating system constraints. A manual collection involves going through the phone manually and photographing each screen individually. It is not very effective, but it is a last resort. The data that may be extracted from a mobile device can be extremely valuable to a case. Messages, call logs, contacts, and photographs are among the most sought-after data sets, but there are several additional pieces of information that might be discovered on a smartphone, including location data, calendar events, notes, and website or application credentials. As a result, mobile device forensic collections are becoming a standard in discovery proceedings. This study aims to implement the mobile forensics technique on Android mobile phones. In order to do this, digital evidence and material data analysis are provided using an example case. It is presumed that an Android smartphone was discovered in this example situation. We installed the utility on Kali. Use Kali's Andriller. All we need to do is connect our Android smartphone and then click "Extract" to obtain the report. We have access to Google Accounts, SMS, Wi-Fi Passwords, Call Logs, Browser History, and other information. With the use of Andriller, a lot of data may be taken from an Android handset and it provided some insight on how to do Android forensics.

Mobile Device Operating Systems
- iOS
- Android
- Windows
- RIM (Blackberry)

Forensic Tools
- ABD
- AFLogical
- OSAF
- Andriller



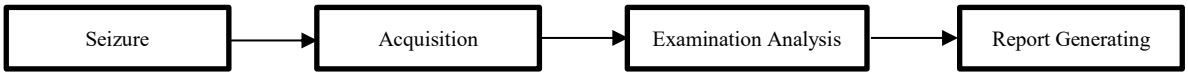
Data Acquisition type
- Manual
- Logical
- Physical

Data Extractions
- Chats/Messages
- Photos/Videos
- Call Logs
- Locations
- Email
- Contacts
- Calendar
- Wee Browsing

Fig. 3. Result and Discussion of Literature Review.

6. The process of mobile forensics

The fact that crimes are not separated from technology trends has made mobile device forensics a crucial component of digital forensic investigations. Digital evidence or relevant data must be recovered from a mobile device in a forensically sound way as the goal of the mobile forensics approach [5]. This can only be accomplished by establishing precise protocols for the collection, transportation, storage, and verification of digital evidence originating from mobile devices as well as for its seizure, isolation, and investigation. Procedures used in other areas of digital forensics are usually transferable to mobile forensics. But be advised that there are unique aspects of the mobile forensics process that need to be considered. In order to get reliable findings from mobile device analysis, it is imperative to follow the correct protocols and standards. The mobile forensics process, the steps:



- Seizure

The purpose of seizing a mobile device at a crime scene is primarily to preserve evidence. Therefore, mobile devices at the crime scene must be seized. Digital forensics adheres to the idea that evidence must always be properly saved, processed, and admissible in court. The confiscation of mobile devices is accompanied by certain legal considerations [38]. There are two key hazards associated with this step of the mobile forensics process: Lock activation (by the user, a suspect, or an unintentional third party), as well as network/cellular connection Network isolation is always recommended, and it may be achieved either by

1. entering airplane mode and disabling Wi-Fi and hotspots or
2. cloning the device's SIM card.

- Acquisition

Acquisition is the second step in mobile forensics and is typically used to retrieve data from the device. A locked display can be unlocked with the correct PIN, password, pattern, or biometric information device. A locked display can be unlocked with the correct PIN, password, pattern, or biometric information. It is difficult to regulate data on mobile devices since the data itself is mobile. Once a smartphone sends communications or files, control is lost. Although there are numerous devices with the capacity to store vast amounts of data, the data itself may be physically located elsewhere. Data synchronization between devices and applications, for instance, can occur both directly and over the cloud [39]. Regardless of the type of device, the fragmentation of operating systems and item specifications might make determining the location of data more difficult. The open-source Android operating system alone is available in a variety of variants, while Apple's iOS may also change between versions. After identifying the data sources, the next step is to correctly gather the data.

- Examination and analysis

Various forensic instruments are utilized to extract data from seized devices [37]. As the initial step in each digital investigation involving mobile devices, the forensic expert must determine:

The type(s) of mobile device(s), such as GPS, smartphone, tablet, etc.

GSM, CDMA, and TDMA Network Type Carrier Service Provider (Reverse Lookup)

The examiner may need to utilize a variety of forensic tools to obtain and analyze the machine's data. Due to the vast variety of mobile devices, there is no universal solution for mobile forensics tools. Since it is impossible to extract all possible information, they must employ two or more inspection tools.

- Report Generating

Upon conclusion of an investigation, the information is frequently given in a nontechnical format. Reports may also contain audit information, and they wonder whether or not the audit has begun. ii) What equipment was used? iii) The current status of the phone. In the end, everything will be processed for a criminal court with a written conclusion of the evidence by an expert. All information, evidence, and other discoveries retrieved, evaluated, and documented during the investigation should be submitted to any other forensic examiner or a court in a clear, succinct, and comprehensive manner [38].

7. Android Architecture

The attractiveness of the Android design is its flexibility with a vast array of devices. This is made possible by the Linux kernel, which is renowned for its interoperability with several hardware platforms. This capability gives manufacturers the flexibility to develop gadgets according to their specifications. Android's adaptability is a significant obstacle for forensic investigators. Therefore, knowing Android's internals and architecture is of utmost importance. The Android platform is constantly evolving. Despite the fact that these modifications substantially alter the architecture, there are basic components that are always static. The Android architecture is comprised of a software stack that comprises an operating system, middleware, and application framework. The software stack consists of four distinct levels [40]. The Linux kernel is fundamental to Android's architecture.

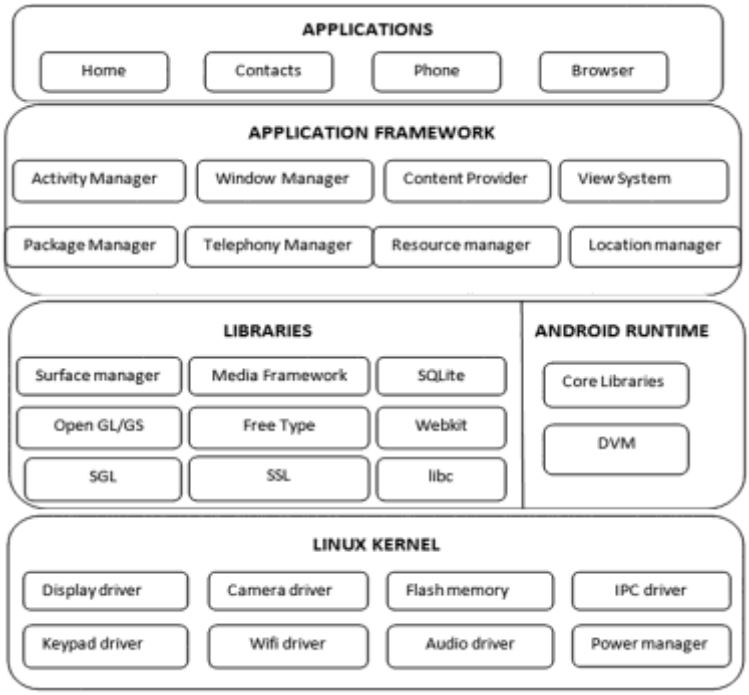


Fig. 4. Android Architecture.

7.1. Android security

Android was developed with a particular emphasis on being secure from the beginning. As a platform, Android provides and enforces various measures that protect the user data that is present on the mobile device through the use of many layers of security [40]. There are a number of secure defaults that will provide protection for the user, as well as a number of services that may be used by the developer community to create secure apps. When deciding how to implement security measures for Android devices, the following considerations need to be given priority:

- safeguarding information about users.
- protecting the available resources inside the system.
- ensuring that a certain application does not have access to the data of another application.

7.2. Android Mobile Device Forensic

Modern mobile phones are commonly referred to as smartphones because they can perform computing tasks and function as miniature computers with limited capabilities. This necessitates an operating system that meets portability requirements. Mobile phones with an open-source operating system allow consumers to freely personalize their devices. This characteristic makes these operating systems very appealing to smartphone manufacturers [6]. Android is the most-used open-source mobile operating system. The Android operating system controls 84.8% of the smartphone market [27].

- The Android File

The great majority of mobile devices running the Android operating system utilize and support the Yet another Flash File System [41]. Additionally, it is very open source.

- The Flash Memories

Flash memory is a nonvolatile solid-state storage device that can function as a read-write memory due to its performance. The two primary types of flash memory are NOR and NAND. In addition, there is a hybrid flash memory

called AND flash that combines the advantages of NOR and NAND. NAND flash memory is optimized for speedy data updates [41].

- Digital Evidence in Android

The partition mtd5 stores third-party apps and all logs created by these applications or the operating system itself [35].

7.3. Data Acquisition Methods in Android Mobile Forensics: Physical & Logical & Manual

Android forensics focuses on extracting data from Android-based devices using sound forensic conditions and legally accepted techniques. The primary tools for forensic capture and analysis of Android-powered devices are described. There are three primary methods for acquiring forensic evidence. Logical and/or physical operations can be used. Logical operations are done exclusively on allotted data and are often executed via file system access. The structure of the file system organizes and provides access to allocated data. Physical operations, on the other hand, deal directly with the physical storage media as opposed to the file system [32-37].

- Manual Acquisition: In this method, a forensic investigator or analyst uses the mobile device's user interface to evaluate the accessible material. The examiner takes photographs of each screen, providing needed information while navigating the gadget. This technique's benefit is that it does not need any tools to acquire data, but its downside is that only data that is accessible to users on the device may be retrieved, and it is time-consuming[39].
- Physical Acquisition: In this method, the data stored on the mobile device is cloned. This method duplicates both deleted data and unallocated space. Following cloning, the cloned data is evaluated using several techniques.
- Logical Acquisition: In this method, neither much manual involvement nor cloning are necessary. Here, data and information accessible on the phone are gathered using automated tools for syncing the phone and PC (typically). The vast majority of free programs perform logical acquisition [15].

This method of acquisition involves cloning or copying the entire physical store bit by bit. The fundamental advantage of physical acquisition is that it permits the study of erased data, portions of data, and unstructured data. Then, tools that do logical acquisition begin by transmitting a sequence of commands from the computer to the mobile device across the established interface [29]. The mobile device responds in accordance with the command request. The answer (data from the mobile device) is transmitted back to the workstation and submitted to the forensic investigator for purposes of report generation. In the majority of cases, an API is utilized to interface with mobile devices. At this level of manual acquisition, it is no longer feasible to restore erased data. When confronted with a broken or missing LCD screen or a damaged or missing keyboard interface, manual extractions have become increasingly challenging, if not impossible. When the gadget is configured to display a language that is unfamiliar to the investigator, it can be difficult to successfully navigate the menu. The following table shows the comparison.

Table 3. Data Acquisition comparison.

Manual Acquisition	Physical Acquisition	Logical Acquisition
SMS	SMS	SMS
data content stored	data content stored	data content stored and Call logs
LCD screen	Call logs	Deleted Files
buttons	Media	Hidden Files
keyboard	App data	Files

Android Digital Forensic Tools

Numerous instruments are at one's disposal for carrying out digital inquiries on Android mobile phones. A few of these solutions support several smartphone platform types and are part of a framework together with other digital forensic tools [35]. The following are the main sources that are utilized to analyze Android devices:

A flexible command-line tool called Android Debug Bridge (ABD) makes it possible to communicate with other Android-powered devices that are connected. During a forensics investigation, the Android platform's debugging mode could be discovered, and the investigator would need to interact with it to extract certain files or verify the value of a certain parameter. The ABD tools are also the main subcomponent that is used by most smartphone forensic

frameworks to communicate with the Android platform. The ABD tool may be used to finish the data collecting phase [26]. Examining malware that is included in Android applications is the main goal of Open Source Android Forensics (OSAF), an open source unified android forensic tool. It follows a set of principles for Android application examination and standards for forensic investigation. Forensic analysis and evidence presentation may be done with OSAF [28].

- Andriller is a smartphone utility that comes with a selection of forensic tools. These utilities' bundles include certain tools with an emphasis on Android forensics. It performs read-only, forensically sound, non-destructive acquisition from Android devices. Further capabilities include bespoke decoders for programs from Android handsets as well as strong lock screen cracking for a pattern, PIN code, or password. In addition to data capture, Andriller can be used for data recovery, forensic analysis, and evidence presentation [6,19].
- AFLogical is an open-source data extraction program that may be used to extract calls, SMS, MMS, MMS portions, and contacts from Android mobile devices. It is accessible on GitHub. It makes a directory with the time and date of the extraction in its name. It can be used in the phases of forensic analysis and evidence presentation.
- SKYPE EXTRACTOR is a tool that may be used to extract data from the Skype application. On an Android phone, it can be used to examine the Skype application. Data such as account information, contact information, calls, chats, file transfers, voicemails, and deleted and changed messages can all be extracted. This program is focused on doing forensic analyses, recovering deleted data, and presenting proof from the Skype application[9].
- WHATSAPP EXTRACT is an open-source tool for extracting and analyzing WhatsApp data. All WhatsApp messages that have been taken from an Android or iPhone device can be seen on an HTML page. WhatsApp is a popular instant messaging service nowadays. This program is focused on the forensic examination and presentation of data from the WhatsApp application [35].

In general, Android forensic tools should be able to look into several kinds of data on an Android smartphone. A sample of the data that can be extracted can be seen in the table 4 [8-12].

Table 4. Sample of extracted data from Android smartphone.

Text messages (SMS/MMS)	Contacts	Call logs	E-mail(Gmail, Exchange) messages Yahoo	Instant Messenger/Chat	GPS coordinates
Photos/Videos	Web history	Search history	Driving directions	Facebook, Twitter, and other social media clients	Files stored on the device
Music collections		Calendar appointments	Financial information	Shopping history	File sharing

7.4. Android Forensic Tools Comparison

The Android forensic tools discussed below are compared to one another in Table 5, which can be found below.

Table 5.Comparison between android tools.

Tools	ABD	OSAF	Andriller	AFLogical	Skype Extractor	Whatsapp Extract
Command lines	√	-	√	-	-	-
GUI	-	√	√	√	√	√
Android OS	√	√	√	√	√	√
Other OS	-	-	√	√	√	√
Support all Apps	√	√	√	√	-	-
Identification	√	√	√	√	-	-
Preservation	√	√	√	√	√	√
Data Recovery	√	√	√	-	√	√
Forensic Analysis	-	√	√	√	√	√
Presentation	-	√	√	√	√	√

Results from the above table show that more phases in the process of performing a digital forensic investigation are covered by Andriller, OSAF, and AFLogical tools. Certain instruments are designed especially for a certain task or procedure. Examples of programs that are specifically designed for WhatsApp and Skype include WhatsApp

Extract and Skype Extract. In light of this comparison, it is evident that Andriller covers more stages than other tools, making it the most complete solution for digital forensics investigation of Android devices.

7.5. Recommendations

Investigators conduct thorough and accurate forensic investigations of Android mobile phones, which can provide valuable evidence in legal proceedings and other investigations. Recommendations for implementing best practices in testing Android mobile phones, supported by references:

Follow standard procedures: It is essential to follow standard procedures for mobile device forensics, such as those established by the National Institute of Standards and Technology or other reputable organizations. These procedures guide data acquisition, analysis, and reporting, as well as the use of appropriate tools and techniques [46].

Use multiple tools and techniques: Using multiple tools and techniques can help ensure the accuracy and completeness of forensic investigations. It is essential to use a variety of tools and techniques to collect and analyze data from the device, including both automated and manual methods [45].

Maintain a chain of custody: It is important to establish and maintain a chain of custody for the device and any data collected from it. The chain of custody should document all individuals who have had access to the device or data, as well as any changes made to the device or data during the investigation [46].

Use verified tools: Use only verified and validated tools for mobile device forensics. Tools should be tested and validated to ensure they are reliable, accurate, and produce repeatable results [45].

Protect the device and data: The integrity of the device and data must be protected during the investigation. This includes protecting the device from physical damage, ensuring that data is not accidentally or intentionally altered or deleted, and ensuring that the device is not infected with malware during the investigation [46].

Document all findings: It is essential to document all findings from the forensic investigation, including the data collected, the analysis performed, and any conclusions drawn from the investigation. This documentation should be clear, concise, and detailed and should be included in the final report [45].

8. IMPLEMENTATION

The ability to comprehend and conduct a forensic test on Android is an essential skill because it is the most popular mobile operating system in the world. We'll look at how to use Andriller to carry out a forensic audit of an Android device.

Andriller is a software package has a selection of forensic capabilities for mobile devices. It performs non-destructive, read-only acquisition from Android devices that is forensically sound. It includes capabilities like strong Lockscreen cracking for Pattern, PIN code, or Password, as well as unique decoders for Apps data from Android (certain Apple iOS & Windows) databases for communications decoding. Reports are generated by extraction and decoders in HTML and Excel formats [34].

8.1. Features of Andriller

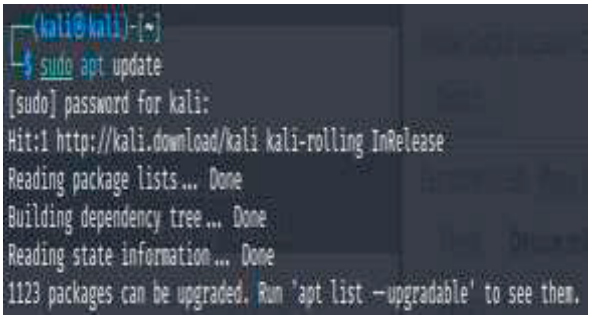
The following are some of the features that Andriller offers for android forensics: -

- automated decoding and data extraction
- Android Backup's data extraction for non-rooted, non-rooted devices (Android versions 4.x, varying/limited compatibility)
- Root ADB daemon, CWM recovery mode, or SU binaries (Superuser/SuperSU) are three options for data extraction with root rights.
- Folder structure, Tarball files (from android backups), and Android Backup data parsing and decoding (backup.ab files)
- Individual database decoders for Android applications selection
- Archive databases for WhatsApp that have been encrypted
- Pattern, PIN, and password lock screen breaking (not gatekeeper)

- Unpacking the Android backup files
- A device's display screen being captured

8.2. Installation on Kali/Parrot Linux

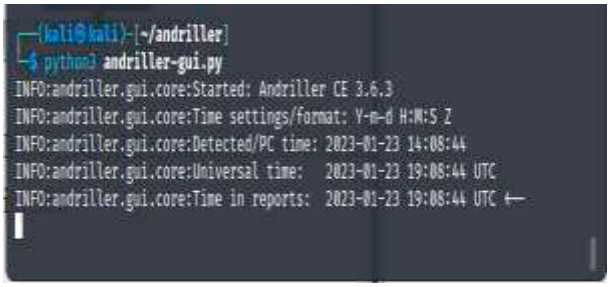
We set up Kali with the utility. Update our Kali system first (recommended), then use the git command to clone the repository from GitHub.



- Let's clone the repository now by using the following command.

- The next three steps:
  - Let's go to the directory: Andriller
  - Need to use the command below to set the permissions for the two files inside the directory.
  - Can run the setup & install Andriller.

- The utility and all of its dependencies are installed using the aforementioned command. The tool may now be used after a successful installation.



All we have to do to acquire the report is click "Extract" after connecting our Android smartphone. Once we have selected "export," we can see that our Android smartphone is prompting us to back up our data. Simply choose "back up my data" to begin.

The reports are automatically opened when the procedure is finished and stored as an html file at the supplied location.

All of the information about the Android smartphone is shown here. We have access to checking Google Accounts, SMS, WiFi Passwords, Call Logs, Browser History, and much more. With the use of Andriller, a lot of data may be taken from an Android handset. and it one of some insight on how to do Android forensics.

As a result, The extraction of data from mobile devices relies heavily on commercially available mobile forensics tools, such as Andriller[40]. This experiment demonstrates that it is possible to manually recover various file formats from a virtual and physical phone. However, problems arise when files are partially overwritten or when the phone's memory is formatted at a low level. Recovery becomes difficult if the file is written in multiple locations.

Andriller is primarily designed for extracting data from Android devices only and does not support iOS devices. Andriller's website and documentation specifically state that the tool is "the most advanced solution for Android phone forensics" and that it "supports more than 11,000 Android devices."

8.3. Open Source Tools Accepted in Court

The acceptability of mobile forensic tools in court may vary depending on jurisdiction and the specific circumstances of the case. In general, courts may consider the reliability, accuracy, and admissibility of the evidence obtained from a mobile forensic tool when determining its acceptability as evidence. Some courts may require that mobile forensic tools be validated and verified to ensure their reliability and accuracy before accepting evidence obtained from them. Additionally, courts may consider the qualifications and expertise of the investigator who used the tool as well as the methodology used to collect and analyze the data. Regarding the acceptability of the Andriller tool specifically, its admissibility as evidence in court may depend on its reliability and accuracy, as well as whether it has been validated and verified by experts in the field. Andriller has been used in a number of forensic investigations and has been cited in academic research [47], suggesting that it may be a reliable tool for mobile device forensics. However, it is ultimately up to the court to determine whether evidence obtained using Andriller or any other mobile forensic tool is admissible in a particular case. It is important for investigators to be aware of the legal requirements and standards for mobile device forensics in their jurisdiction and to use only verified and validated tools and methods to ensure the accuracy and reliability of the evidence obtained.

9. Cloud Forensics in Android Devices

As the prevalence of cloud storage services continues to rise, the need for robust methodologies for conducting cloud forensics on Android devices becomes imperative. Cloud forensics involves the acquisition, analysis, and interpretation of digital evidence stored in cloud storage services used by Android devices, such as Google Drive and Dropbox [11]. Cloud storage services are characterized by complex storage architectures, distributed data replication, and encryption mechanisms [2]. Extracting and analyzing data from these services requires specialized techniques

tailored to their unique characteristics. Acquiring data from cloud storage services necessitates understanding the underlying storage architecture and security mechanisms employed by the service providers. Techniques such as API-based data extraction, reverse engineering of client applications, and analysis of synchronization artifacts can be explored to obtain relevant data from the cloud [1]. Then, cloud-stored data may be fragmented or partially available due to the distributed nature of cloud storage systems. In the future, focus will be on developing robust techniques for data reconstruction, including data deduplication, metadata analysis, and data carving, to ensure the integrity and completeness of acquired evidence [24]. Cloud storage services often employ encryption mechanisms to protect user data. Decrypting encrypted data and recovering encryption keys are crucial tasks in cloud forensics [3]. In addition, analyzing metadata and correlating it with other digital evidence can aid in establishing a comprehensive picture of events and user interactions within the cloud environment [43]. Cloud forensics on Android devices presents unique challenges due to the distributed nature of cloud storage services and the encryption mechanisms employed. Future research should focus on developing and advancing techniques for data acquisition, reconstruction, encryption handling, metadata analysis, and addressing legal and privacy considerations [15].

10. Conclusions and Future Work

Mobile forensics, or digital forensic investigation for mobile devices, is the fastest-evolving and fastest-growing digital forensic specialization. Any device's digital forensic procedure begins with identification, data collection, data recovery, forensic analysis, and evidence presentation. Android, a platform for mobile devices, has dominated the smartphone market. Therefore, any expert in digital forensics must undertake the crucial task of developing techniques for digitally analyzing Android smartphones. This article describes the fundamental functionality of mobile devices, demonstrates how they can be used as sources of digital evidence, and provides tools and methodologies for collecting and analyzing digital evidence on these devices. In addition, the article provides an explanation of mobile devices' fundamental functionality. However, selecting the proper instrument to conduct digital investigative procedures requires knowledge of the Android smartphone's software and hardware architecture. In the realm of Android forensics, numerous solutions are readily available to manage the various phases of the digital investigation process. morevor, This paper demonstrates a portion of the tools that can be used to manage the investigation process and provides a starting point for the development of a framework that adheres to the standard digital forensic procedures for Android mobile devices. Despite the fact that the Andriller application was used to collect digital evidence from an Android smartphone, Android operating systems were used for the digital forensics instruments in this investigation, as mentioned previously. This paper proposes future enhancements for Andriller to improve its effectiveness in Android forensic investigations. The suggested enhancements may include advancements in data extraction techniques, compatibility with new Android versions, support for additional data types, integration with advanced analysis methods, and addressing identified limitations. These enhancements aim to enhance the capabilities of Andriller for better forensic analysis of Android devices. Also, to improve the efficiency of digital forensic investigations on Android devices, advancements in data extraction techniques are required. In addition, as more users store their data in the cloud, it is imperative to develop robust methodologies for conducting cloud forensics on Android devices. in the future should explore techniques for acquiring and analyzing data from cloud storage services utilized by Android devices, such as Google Drive and Dropbox.

Ethical Approval: Not Applicable.

Competing Interest: There is no competing interest. This is student's research paper. If it get accepted and then published then it will be good for student's research.

Authors' Contributions: All authors equally contributed.

Funding: This paper was funded by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia under the [GRANT_ _].

Availability of Data and Materials: Not applicable.

Acknowledgments: The authors extend their appreciation to the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia [GRANT _ _]. The authors would like to thank the anonymous reviewers for their insightful scholastic comments and suggestions, which

11. References

1. Sunde, N., & Horsman, G. (2021). Forensic Science International: Digital Investigation. Forensic Science International, 36, 301074.
2. Goel, A., Tyagi, A., & Agarwal, A. (2023). Smartphone forensic investigation process model. Computer Science Journals (CSC Journals).
3. Kohn, M. D., Eloff, M. M., & Eloff, J. H. P. (2013). Integrated digital forensic process model. Computers & Security, 38, 103–115
4. Varol, C., & Tayeb, H. F. (2023). Android Mobile Device Forensics: A Review. Cloudfront.net.
5. Parikh, T. S., & Lazowska, E. D. (2006). Designing an architecture for delivering mobile information services to the rural developing world. Proceedings of the 15th International Conference on World Wide Web.
6. (2023).
7. Bang, J., Lee, Y., Lee, Y.-T., & Park, W. (2019). AR/VR based smart policing for fast response to crimes in safe city. 2019 IEEE International Symposium on Mixed and Augmented Reality Adjunct (ISMAR-Adjunct), 470–475.
8. Casey, E., & Turnbull, B. (2023). Digital Evidence on Mobile Devices. Elsevier.com.
9. Casadei, F., Savoldi, A., & Gubian, P. (2023). Forensics and SIM cards: An overview. Utica.edu.
10. Novak, M., Grier, J., & Gonzales, D. (2023). New approaches to digital evidence acquisition and analysis. Ojp.gov.
11. Pribadi, B., Rosdiana, S., & Arifin, S. (2023). Digital forensics on facebook messenger application in an android smartphone based on NIST SP 800-101 R1 to reveal digital crime cases. Procedia Computer Science, 216, 161–167.
12. Da Naing, A. T., Guan, J. S. B., Win, Y. S., & Pan, J. (2023). A review on the effectiveness of dimensional reduction with Computational Forensics: An application on malware analysis. ArXiv [Cs.CR].
13. Silalahi, S., Ahmad, T., & Studiawan, H. (2023). Transformer-based named entity recognition on drone flight logs to support forensic investigation. IEEE Access: Practical Innovations, Open Solutions, 11, 3257–3274.
14. Saranya, S., & Usha, G. (2022). Forensic analysis of online social network data in crime scene investigation. In Artificial Intelligence and Blockchain in Digital Forensics (1st Edition, pp. 183–209). River Publishers.
15. Zhang, Y., Li, Y., & Li, Z. (2023). Aye: A trusted forensic method for firmware tampering attacks. Symmetry, 15(1), 145.
16. Shin, Y., Kim, S., Jo, W., & Shon, T. (2022). Digital forensic case studies for in-vehicle infotainment systems using Android Auto and Apple CarPlay. Sensors (Basel, Switzerland), 22(19), 7196.
17. Mirza, M. M., Ozer, A., & Karabiyik, U. (2022). Mobile cyber forensic investigations of Web3 wallets on Android and iOS. Applied Sciences (Basel, Switzerland), 12(21), 11180.
18. Kim, H., Shin, Y., Kim, S., Jo, W., Kim, M., & Shon, T. (2022). Digital forensic analysis to improve user privacy on Android. Sensors (Basel, Switzerland), 22(11), 3971.
19. Hutchinson, S., Mirza, M. M., West, N., Karabiyik, U., Rogers, M. K., Mukherjee, T., Aggarwal, S., Chung, H., & Pettus-Davis, C. (2022). Investigating wearable fitness applications: Data privacy and digital forensics analysis on Android. Applied Sciences (Basel, Switzerland), 12(19), 9747.
20. Salimi, N. F., Abd Warif, N. B., & N Ismail, N. S. (2022). Comparative analysis of logical acquisition using Wondershare Dr. Fone, MOBILedit Forensic, and FonePaw on android phones / Nuraimi Farhana Salimi, Nor Bakiah Abd Warif and Nor-Syahidatul N Ismail. Malaysian Journal of Computing (MJoC), 7(2), 1162–1177.
21. Younis, L. B., Sweda, S., & Alzu'bi, A. (2021). Forensics analysis of private web browsing using android memory acquisition. 2021 12th International Conference on Information and Communication Systems (ICICS).
22. Ceballos Delgado, A. A., Glisson, W. B., Grispos, G., & Choo, K.-K. R. (2022). FADE : A forensic image generator for android device education. WIREs Forensic Science, 4(2).
23. Fernando, V. (2021). Cyber forensics tools: A review on mechanism and emerging challenges. 2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 1–7.
24. Bharath Bhushan, H. H., & Metilda Florance, S. (2022). An overview on handling anti forensic issues in android devices using forensic automator tool. 2022 IEEE International Conference on Signal Processing, Informatics, Communication and Energy Systems (SPICES), 1, 425–430.
25. Tayeb, H. F., & Varol, C. (2019). Android Mobile Device Forensics: A Review. 2019 7th International Symposium on Digital Forensics and Security (ISDFS), 1–7.
26. Kim, D., & Lee, S. (2020). Study of identifying and managing the potential evidence for effective Android forensics. Forensic Science International: Digital Investigation, 33(200897), 200897.

27. Almehmadi, T., & Batarfi, O. (2019). Impact of android phone rooting on user data integrity in mobile forensics. 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), 1–6.
28. Al-Dhaqm, A., Razak, S. A., Ikuesan, R. A., Kebande, V. R., & Siddique, K. (2020). A review of mobile forensic investigation process models. IEEE Access: Practical Innovations, Open Solutions, 8, 173359–173375.
29. Hermawan, T., Suryanto, Y., Alief, F., & Roselina, L. (2020). Android forensic tools analysis for unsend chat on social media. 2020 3rd International Seminar on Research of Information Technology and Intelligent Systems (ISRITI), 233–238.
30. Mirza, Mohammad M., Salamh, F. E., & Karabiyik, U. (2020). An android case study on technical anti-forensic challenges of WhatsApp application. 2020 8th International Symposium on Digital Forensics and Security (ISDFS), 1–6.
31. Riadi, I., Umar, R., & Firdonsyah, A. (2017). Identification Of Digital Evidence On Android's Blackberry Messenger Using NIST Mobile Forensic Method. International Journal of Computer Science and Information Security (IJCSIS), 15(5), 3-8.
32. FEBRIANSYAH, L. (2018). ANALISIS KETERLIBATAN CYBERTERORISM MENGGUNAKAN METODE ANALITYCAL HIERARCHY PROCESS (AHP) (Master's thesis, Universitas Islam Indonesia).
33. Alhassan, J. K., Oguntoye, R. T., Misra, S., Adewumi, A., Maskeliūnas, R., & Damaševičius, R. (2018). Comparative evaluation of mobile forensic tools. In Proceedings of the International Conference on Information Technology & Systems (ICITS 2018) (pp. 105–114). Springer International Publishing.
34. Acharya, S., Rawat, U., & Bhatnagar, R. (2022). A comprehensive review of Android security: Threats, vulnerabilities, malware detection, and analysis. Security and Communication Networks.
35. Maria Jones, G., Godfrey Winster, S., & Scholar, P. G. (2023). Forensics analysis on smart phones using mobile forensics tools. Ripublication.com.
36. Hoelz, H., Herdl, C., Gerstl, L., Tacke, M., Vill, K., von Stuelpnagel, C., Rost, I., Hoertnagel, K., Abicht, A., Hollizeck, S., Larsen, L. H. G., & Borggraefe, I. (2020). Impact on clinical decision making of next-generation sequencing in pediatric epilepsy in a tertiary epilepsy referral center. Clinical EEG and Neuroscience: Official Journal of the EEG and Clinical Neuroscience Society (ENCS), 51(1), 61–69.
37. Mayrhofer, R., Stoep, J. V., Brubaker, C., & Kralevich, N. (2021). The Android platform security model. ACM Transactions on Privacy and Security, 24(3), 1–35.
38. Fukami, A., Stoykova, R., & Geradts, Z. (2021). A new model for forensic data extraction from encrypted mobile devices. Forensic Science International: Digital Investigation, 38(301169), 301169.
39. Kumar Agrawal, A., Sharma, A., & Khatri, P. (2019). Android forensics: Tools and techniques for manual data extraction. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3356336
40. Jones, G. M., & Winster, S. (2017). Forensics analysis on smart phones using mobile forensics tools.
41. Casey, E. (2021). Digital evidence and computer crime: Forensic science, computers, and the internet (4th ed.). Academic Press.
42. National Institute of Justice. (2017). Electronic crime scene investigation: A guide for first responders.
43. National Institute of Standards and Technology. (2016). NIST Special Publication 800-86: Guide to Integrating Forensic Techniques into Incident Response.
44. Casey, E. (2018). Handbook of digital forensics of multimedia data and devices. John Wiley & Sons.
45. National Institute of Standards and Technology (NIST). (2020). Special publication 800-204. Guide to forensic analysis of mobile devices.
46. Sharma, A., Singh, J., & Kumar, N. (2021). A review of Android Smartphone Forensic Analysis Tools. International Journal of Advanced Science and Technology, 30(2), 3592-3600.