ISSN: 2182-2069 / E-ISSN: 2182-2077

Unlocking Digital Evidence: Recent Challenges and Strategies in Mobile Device Forensic Analysis

Bandr Fakiha[1*]

[1*]Associate Professor, Faculty of Health Sciences, Department of Medical Health Services, Umm Al-Qura University, Saudi Arabia. bsfakiha@uqu.edu.sa, https://orcid.org/0009-0006-7537-0251

Received: December 19, 2023; Revised: February 06, 2024; Accepted: March 09, 2024; Published: May 30, 2024

Abstract

We live in a digital era where communication has become easier than ever, thanks to the emergence of computer technologies. With the improvement of these technologies over the last few decades, mobile devices have evolved and advanced, offering users fast and affordable ways to interact virtually. Forensic investigators have learned to take advantage of mobile device technologies to unveil digital evidence. This paper delves into the challenges and techniques involved in conducting forensic analysis on mobile devices. It also explores the logical extraction and analysis of data from mobile devices. Although it can be limited by the device's safety features or encryption, logical extraction entails connecting the mobile device to computers and using software programs to gain entry to and copy files stored in the gadget's file system. It highlights crucial advancements and the secrets surrounding this field with the primary objective of establishing more facts on the modern world of digital forensic investigation. Device heterogeneity, data fragmentation, cloud and synchronization, privacy, and legal considerations were found to be the most common challenges in forensic analysis. Device heterogeneity is where the computers run separate operating systems or the devices are manufactured by different companies. You are probably familiar with both the Internet and cell phone networks, which are two typical instances of heterogeneous networks. The Internet and cell phone networks are two popular instances of heterogeneous networks that you are probably already familiar with. Device exploitation, password cracking, file carving, database reconstruction, leveraging APIs, and obtaining legal cooperation were the preferred techniques involved in the analysis. On the other hand, decryption, advanced data carving, keyword searching, and data filtering are some of the crucial advancements in mobile device forensic tools. The results imply a dire need for a complex landscape to preserve data integrity throughout digital forensic investigations. The researcher uses this study's findings to recommend future action plans for stakeholders, including digital forensic investigators and the general public.

Keywords: Forensic Analysis, Mobile Devices, Digital Evidence, Data Extraction, Security Threats.

1 Introduction

Background and Context of the Study

In the present digital era, the rapid growth of computer technologies has completely transformed communication, making it more practical and available than before. Several computer-related

DOI: *10.58346/JISIS.2024.I2.005*

*Corresponding author: Associate Professor, Faculty of Health Sciences, Department of Medical Health Services, Umm Al-Qura University, Saudi Arabia.

technologies have emerged over the last few decades. Particularly, mobile devices have seen significant development, which has led to the provision of consumers with quick and affordable methods to connect and communicate more effectively. Consequently, mobile device forensic analysis has emerged as a result of forensic investigators starting to realize the enormous potential of mobile devices as valuable sources of digital evidence (Abdulaziz et al., 2023).

The field of mobile device forensic analysis involves the extraction, preservation, and analysis of data stored within mobile devices (Fukami et al., 2021). These devices have become a crucial part of both our personal and professional lives, and they contain a lot of crucial data, such as text messages, call logs, application data, and geolocation data, that can be very beneficial in forensic investigations (Aljahdali et al., 2021). Typically, resource shortages, inexperience, irritation with the amount of data, and expectations imposed by forensic science and technology (FST) are some of the difficulties and restrictions faced by forensic technology. However, carrying out forensic analysis on mobile devices has other numerous unique challenges that forensic investigators need to overcome in their operations. For instance, a wide range of mobile device models, operating systems, and versions makes the forensic procedure more difficult, demanding investigators' significant training and experience to efficiently extract and analyze evidence (Da Silveira et al., 2020). In computer forensics, digital evidence preservation is essential (Stoyanova et al., 2020). Start by recording specifics like the location and method of evidence collecting. The investigators are required to keep the chain of custody safe. They must also produce forensic pictures to guarantee a precise replica of the storage media. This process of recovery and preservation have become more complicated by the use of encryption methods, data fragmentation, and synchronization with cloud services used by modern mobile devices. With the fast spread of mobile devices and our growing reliance on digital communication and data storage, cybercrimes have increased dramatically and calls for better methods of evidence analysis. However, regarding mobile devices, the mere diverse nature of models and operating systems is one of the most common challenges in the field that complicates the forensic process (Afzal et al., 2019). Forensic investigators may have to grapple with compatibility and inconsistency issues, considering the mammoth of device models and their versions that exist in the market. Consider the data from StatCounter GlobalStats: as of January 2022, it indicated that there are approximately 3.5 billion mobile devices and the market share of the Android mobile operating system across the globe is at 71%, while that of iOS is approximately 27%.

Every operating system is versioned, and there is a variant in use by the various device manufacturers; it, therefore, becomes more complicated to analyze forensically. For example, much fragmentation is contributed when every manufacturer makes a variety of products but with unique versions of the Android operating system. This is now very hard for forensic tools and techniques to keep up with because the landscape keeps changing. Recent examples highlight the complexity and diversity of mobile devices encountered in forensic investigations. In another event, say, criminal or terrorist activities, cybercrime, corporate espionage—the forensic analysts would have to deal with, in all probability, the greatest number and wide variety of mobile devices used by the subjects and possess each with their peculiar features and security settings. For example, during the investigation after the San Bernardino shooting in 2015, the FBI did not have easy access to encrypted data stored in one of the attackers' used iPhone 5C. The case raised an even more considerable legal and technical debate over privacy rights, encryption, what obligations the technology companies should have, and how to help law enforcement with access to encrypted data. Herein, the incidents point to the challenges of the diversified nature of mobile devices and the requirement for an innovative solution so that the noted hindrances in terms of forensic investigation can be met. A second major obstacle to mobile device forensic analysis is data fragmentation (Al-Dhaqm et al., 2020). Data stored on mobile devices is dispersed and fractured, making it challenging to reassemble a complete data collection. This fragmentation hampers the ability of forensic investigators to retrieve and analyze digital evidence cohesively (Sumithra & Sakshi, 2024).

Privacy and legal considerations are another important factor that involves conducting the test in a legal and moral manner that will ensure adherence to legal obligations, the right to consent, and, more importantly, the privacy and reliability of the data obtained (Ferguson et al., 2020). One might argue that since the role played by mobile technologies in many dimensions of modern life has been increasing, it follows that the associated unique barriers, strategies, innovations, and vulnerabilities peculiar to mobile device forensics must be developed. This research will try to explore these issues and bring out useful information that may enlighten forensic investigators, digital forensic tool creators, legal representatives, and other participants in this field.

Relevance and Nature of the Study

This study contributes to the modern scientific world because of the increasing prevalence of mobile devices and the importance of those devices in modern-day forensic investigations. Mobile devices have, in recent years, become a crucial aspect of both our day-to-day lives. This phenomenon renders them potential sources of crucial digital evidence in several criminal acts. The most common ones are fraud and online misconduct or cybercrime (Sunde & Dror, 2019). As it is, forensic investigators, law professionals, legislators, and even the general public need to be aware of the challenges and methods that are encountered in performing forensic analysis on mobile devices in order to help contribute to more accurate and efficient analysis of digital evidence in the future (Ryu et al., 2019).

The research results may help to build improved methods and procedures. These improvements may help increase the effectiveness of forensic investigations that involve mobile devices. Forensic investigators can choose and use the best tools for extracting, preserving, and analyzing digital evidence from mobile devices by having a thorough awareness of the strengths and weaknesses of various technologies. Furthermore, ongoing investigation and study are undeniably crucial due to the constantly changing landscape of mobile security risks.

The research, in the process, further enhances the understanding of forensic implications to be put in place properly for countermeasures in dealing with mobile security events based on the nature and influence of those risks on mobile device forensic analysis (Casey, 2019). This is a character study with further use of the case study and observation as the main data-gathering techniques for the main character's activities, actions, decisions, and behavioral patterns throughout the case study. Case analyses presented in this book are real cases from practical experience and will, therefore, provide invaluable insight into the difficulties the forensic investigator comes up with and ways to surmount them. The study contributes to the pool of knowledge already available in the area of mobile device forensic investigation and serves as a resource for those working in digital forensics, legislators, attorneys, and the general public.

Research Aim

The basic aim of my study is to uncover the nature of prevalent challenges and methods involved in conducting forensic analysis on mobile devices. I seek to illuminate the present state of forensic examinations by exploring the processing and extraction of data from these devices. The researcher plans to achieve this by looking into both the difficulties encountered and advancements made in mobile device forensic technologies. Moreover, this research plans to contribute to the pool of knowledge about digital forensic investigations by shedding light on the techniques and developments in mobile device forensics. The knowledge gained from this study will be a useful tool for digital forensic investigators, assisting them in navigating the obstacles of mobile device forensic analysis and maintaining data integrity throughout the course of the investigation. Furthermore, the study's recommendations will assist different parties involved in mobile device forensic analysis in developing future action plans, ensuring continuing progress in this vital field of digital forensics.

Research Objectives

The researcher also devised the objectives below to ensure he covered every research aspect according to the research needs.

- To identify and analyze the key challenges faced by forensic investigators in conducting analysis on mobile devices.
- To explore and evaluate the techniques employed in conducting forensic analysis on mobile devices.
- To investigate the evolving landscape of mobile security threats and their implications for mobile device forensic analysis.
- To examine the advancements in mobile device forensic tools and technologies.
- Based on the research results, provide recommendations and future action plans for digital forensic investigators, policymakers, and the general public.

2 Literature Review

Unique Challenges and Techniques Involved in Conducting Forensic Analysis on Mobile Devices

When conducting analyses to obtain digital evidence, forensic investigators encounter challenges like heterogeneous device types, data fragmentation, difficult cloud and synchronization processes, and privacy and regulatory issues (Casino et al., 2022; Hou et al., 2013; Muralidharan, 2020). Device heterogeneity refers to mobile devices coming in numerous models, operating systems, and versions (Fukami et al., 2021; Abinaya et al., 2014). The mechanisms of storage within these gadgets, the file systems, and even the encryption protocols are bound to be variant. These diversities, therefore, add to the complexity of forensic investigation to ensure the accurate retrieval of digital evidence (Lee & Woo, 2022). It requires special knowledge and experience in handling and extracting data from diverse devices. The other aspect of data fragmentation is that data is dispersed and floats in different storage locations over portable devices (Lim et al., 2019. Typically, Cloud platforms provide options for storing data. Effective data preservation, analysis, and collaboration are made possible by it, guaranteeing successful criminal investigations and prosecutions. However, (Bouchaud et al., 2021; Ram & Chakraborty, 2024; Pakkiraiah & Satyanarayana, 2024) argue that the proliferation of digital devices and the increasing reliance on cloud services have exponentially expanded the sources of fragmented data and exacerbated this challenge. With data spread across diverse platforms such as cloud storage, external drives, SIM cards, and device memory, reconstructing a coherent data set demands intricate expertise and sophisticated tools. A report by the International Data Corporation indicated that the volume of data worldwide is expected to reach 175 zettabytes by 2025. It exacerbates the fragmentation issue, as the sheer volume of data increases the likelihood of dispersion across multiple platforms. For instance, the SolarWinds cyberattack in 2020, attributed to state-sponsored actors, compromised numerous organizations by infiltrating their IT management software. Forensic investigators faced the daunting task of sifting through disparate data sources to understand the extent of the breach and attribute responsibility. Also, the NCSC in 2016 urged the sports industry to strengthen its defenses in a report it released in July that detailed several hitherto unreported security problems in England. In fact, one of the most famous football teams in the world, Manchester United, and other sports leagues have recently been attacked by cybercriminals (Atlam et al., 2020). The NCSC surveyed 57 sporting groups and found that 70% had at least one "attack" every year. The report further mentions that investigators handling these cases had faced the challenge of gathering evidence against the crimes, as evidence was spread across different systems within the organizations and their partner companies.

Moreover, legal and privacy considerations further complicate the process of data reconstruction because compliance with regulations such as the General Data Protection Regulation (GDPR) imposes strict requirements on handling personal data that call for meticulous attention to detail in data gathering and analysis. The exploitation of AI in generating videos (deepfakes) is an example of a situation demanding improved knowledge. AI, in particular, is an emerging technology that demands advanced proficiency, given its potential to disrupt the legal systems surrounding the use of digital resources (Atlam et al., 2020).

The issue of regulations is also witnessed in the analysis phase, given that there has been an increasing concern on the sensitivity of data often stored in people’s devices and investigators have been scrutinized in the past over the issue of privacy (Sayakkara et al., 2019). Forensic investigators, therefore, have to face these special challenges through numerous ways to locate, store, and analyze the digital evidence that the particularities of the mobile device forensic investigation pose. The exploitable device, therefore, involves the process of finding and exploiting the loopholes in mobile devices to be able to access the extractive data (Harkin et al., 2020). These are methodologies that facilitate the investigator to avail themselves of pertinent digital evidence to a case, according to (Marques et al., 2019). Recently, statistics showed that the exploitation of mobile devices was increasing; cyber criminals increasingly view smartphones and tablets as very lucrative attack vectors. A report (Roumani, 2020) found that mobile devices were involved in 20% of data breaches in 2020. Moreover, the proliferation of mobile malware continues to pose a significant challenge for cybersecurity professionals, with over 5.2 billion malicious installation attempts detected in 2020 alone (Roumani, 2020). A program or piece of code, known as an exploit, is made specifically to identify and take advantage of a security hole or weakness in a computer system or application. Usually, this is done for malevolent intents like installing malware. An exploit is not malware; rather, it is a tool used by cybercriminals to distribute malware. It depends on the discovery of security flaws in the operating system or firmware of mobile devices, which can be exploited to bypass security mechanisms and gain elevated privileges. Once a vulnerability is identified, the investigator can deploy various techniques, such as malware injection, privilege escalation, or remote code execution, to compromise the device and access sensitive information stored within it. Common attack vectors used by malicious actors include phishing attacks and network-based exploits targeting known vulnerabilities. Recent examples of device exploitation include the use of sophisticated malware like Pegasus, developed by the NSO Group, which has been used to target high-profile individuals, activists, and journalists worldwide (Rudie, 2021). Pegasus exploits zero-day vulnerabilities in mobile operating systems such as iOS and Android to covertly infect devices and exfiltrate sensitive data like messages, calls, emails, and location information. Investigators in different parts of the world are using this technique to learn from captured criminals and obtain relevant evidence from mobile devices that cannot be accessed through the original user.

Password cracking is the second method. Forensic investigators use password-cracking techniques to understand passcodes, patterns, and facial or other biometric locks securing mobile devices. These methods make use of dictionary attacks, brute-force attacks, or flaws in password security measures. Password cracking is an essential tool that has long been utilized by investigators. Often, it starts with the use of dictionary attacks, which rely on pre-existing word lists or dictionaries containing commonly used passwords, phrases, or character combinations. Such lists are accessed in a systematized manner and compared with the encryption of the password stored either on a device or a server. One has just to locate a match, and the attacker is given easy access without having to decrypt the password. This, however, always meets users who have complex and unique passwords that cannot be easily guessed from the dictionary. Nonetheless, such methods as a dictionary attack are still very effective, mostly with the majority of users who use simple or commonly used passwords. For example, one of the simplest passwords turned out to be "123456" and "password" in a National Institute of Standards and Technology (NIST) study in 2020 (Ertam et al., 2023).

Brute-force attacks involves systematically trying every possible combination of characters until the correct password is discovered. It is more time-consuming and resource-intensive than dictionary attacks as it does not rely on predefined word lists. They have always been effective against passwords with weak complexity requirements or shorter lengths. For example, in 2019, the cybersecurity firm Syhunt reported that 15% of passwords in a sample set were six characters or shorter, making them susceptible to brute-force attacks. Organizations often enforce stronger password policies, such as requiring longer passwords with a mix of alphanumeric characters and symbols, as well as implementing account lockout mechanisms to prevent multiple login attempts.

Attacks against password weaknesses often involve features of the related security, such as hashing algorithms or encryption protocols, considering the strength as a means to defeat authentication mechanisms and obtain plaintext passwords. For example, cryptographic algorithm weaknesses at the level of MD5 or SHA-1 would tend to bring cases in which the hashed representations of the password could have been recovered to plain text. Similarly, the weak authentication protocol is available to an attacker for the easy cracking of the password, which contains insufficient entropy or predictable generation of the password. Thirdly, file carving is used to recover erased or fragmented data from mobile devices (Cantrell, 2019).

Generally, the evidence in both the unallocated and damaged storage regions is reconstructed using some special software tools that identify or carve files by their headers, footers, or any other specific signature. Fourthly, structured data storage is a common use of the database by mobile gadgets (Azad et al., 2020). In practice, the methods of database reconstruction allow the investigators to recover and evaluate data found in those databases. This involves understanding the layout of the database, running SQL queries, and obtaining relevant information for forensic investigation. Investigators use Application Programming Interfaces (APIs) offered by cloud service providers to access data stored in the cloud. These APIs enable the forensically sound gathering of data from cloud platforms. Software systems that already exist can be integrated with new applications using APIs. As a result, development can go more quickly because no feature needs to be created from start. APIs allow you to utilize pre-written code. Additionally, legal cooperation, such as warrants or subpoenas, is essential in order to access cloud-based data and guarantee its acceptability in court proceedings (Wright, 2019). The techniques have long been used to overcome numerous techniques in this field. However, it is essential to continuously adapt and enhance these strategies as mobile technology develops and security measures become more sophisticated.

Extraction and Analysis of Data from Devices

In forensic investigations, data extraction and analysis from smartphones, tablets, wearables, and IoT devices are essential because they provide valuable digital evidence. Investigators typically, choose the technique based on the features and the general nature of the device in question. Also, the objective or goal of the investigation is always considered (Wright, 2019). Logical extraction which involves accessing data via the device's operating system or applications is often used to access elements like call logs or multimedia files. Physical extraction entails producing a bit-by-bit replica of the storage on the device. The process of extracting useful data from a mobile device, such as a tablet or phone, is known as logical extraction and the good thing about it is that it is simpler than the others (Khan et al., 2020). After the data has been recovered, forensic analysts use several techniques to analyze it. Understanding user actions, creating timelines, and discovering connections all depend on metadata analysis. Time stamps, location data, and device identifiers are examples of metadata that offer helpful insights. Groß (2022) mentions that data carving techniques are used to recover deleted or fragmented files from unallocated or damaged storage spaces. Analysts can reconstruct files and compile evidence by recognizing file signatures or certain file headers and footers. A distinct identification number that appears at the start of a file is called a file signature. It gives you details about the data it contains as well as the type of file. It tells a computer what program to use to open it or how to read it. In order to find trends, contacts, and communication networks, data analysis may also consider looking into communication data, such as call logs and text messages.

Analyzing application data is extracting information from installed programs such as messaging services, social networking sites, and productivity tools. It can bring to light user interactions, shared media, and conversations. Devices like IoT and wearables are the base used in the data collection and analytic framework (Connolly & Wall, 2019). For example, the wearables of this category could be smartwatches and fitness trackers, which collect location details, user logs of activity, and other data related to health. The forensic examination of wearable activities involves the acquisition and analysis of the activities in order to reconstruct events or patterns of activity. Specifically, sensor data, GPS coordinates, and health-related indicators. IoT gadgets produce an enormous amount of data, given that they are connected to other devices, such as autonomous vehicles and smart home appliances. Understanding sensor readings, connection protocols, as well as these device setups requires specialist knowledge and tools to enable effective and detailed extraction and analysis of data from IoT devices.

Developments in Mobile Device Forensic Tools and the Changes in Mobile Security Threats Landscape

Several researchers in this field have published numerous developments in the industry. Siriwardhana et al., (2021) argue that advancements in mobile device forensic tools have played an instrumental part in addressing challenges related to digital evidence analysis. Emerging technologies in digital forensics, such as artificial intelligence (AI) and machine learning (ML), perform tasks like text, image, voice, and behavior analysis (Jelena et al., 2023). AI and ML are quickly replacing manual labor as vital tools in the digital forensic toolbox because they speed up investigations and reduce manual work. Some other noticeable developments include enhanced data retrieval abilities in mobile device forensic tools, which allow investigators to retrieve data from a wide range of device types and models. Miloslavskaya & Tolstoy (2019) argue that these tools support physical, logical, and file system extractions, hence enabling the acquisition of comprehensive data sets from numerous mobile devices.

There is also advanced social media and program analysis. Several sources argue that the ability of mobile device forensic tools to handle app and social media data has increased over the last few years. Investigators can acquire app data, chat records, multimedia files, and location data, giving them insights into user behavior and habits. Mobile device forensics may routinely recover deleted or buried data from a device, providing vital evidence for an investigation. A rigorous process is followed to make sure that the data gathered by investigators is admissible in court. Social media forensics collects information from networks like Facebook in order to identify perpetrators. Most forensic tools can confirm if a file's signature is different from what is expected based on its extension. A precompiled database can be used to verify the signature of the file. After determining whether the signature is present, the related extension will be looked up. Accurate data is recovered and preserved with the aid of other mobile forensic technologies.

Along with improvements in forensic technologies, investigators continue to face difficulties due to the changing nature of mobile security risks, as malware, spyware, phishing attempts, network breaches, and device tampering become more rampant. These are just but a few of the risks that mobile devices are susceptible to. Mobile devices have become a point of entry into companies for data theft or attack creation. Mobile Security is crucial since it may foresee risks such as malware, phishing scams, dangerous mobile applications, data leaks, identity theft, and many more. Security experts have always emphasized that some of the most effective ways to prevent the consequences of cybercrime and assist investigators in gathering digital evidence include installing reputable antivirus software, keeping devices and apps up to date, and avoiding phishing and spam by being wary of unsolicited messages, avoiding clicking on dubious links, and establishing the authenticity of communication before distributing sensitive information.

Al-Turjman & Salama, (2021) argue that forensic investigations have become more challenging since advanced persistent threats (APTs) began targeting mobile platforms. Mobile device forensic analysis needs to undergo ongoing study and improvement to keep up with the methods employed by malicious actors. The creation of proactive security measures and countermeasures is also required due to the changing nature of mobile security threats. Forensic investigators must modify their methods to identify and respond to the constantly evolving threat environment. This involves staying updated on emerging threats, collaborating with cybersecurity experts, and continuously refining forensic methodologies hence addressing the challenges posed by evolving mobile security threats. These tools provide enhanced data extraction capabilities, cloud data acquisition features, improved app and social media analysis, and malware detection capabilities.

Gaps in Literature and Research Needs

Much has been investigated and published about challenges and advancements in forensic data analysis on mobile devices. However, several notable gaps require further research and investigation to shed more light on the issue, not only to contribute to the existing literature but also to help different parties solve related issues. The most significant gap that requires further exploration is that there is little study on the forensics of IoT devices. There is a substantial research deficit regarding the topic of IoT device forensics, despite smartphones, tablets, and wearables having attracted a lot of attention in the field of mobile device forensics. IoT devices, such as connected cars and smart home appliances, provide a significant amount of data that can be used in forensic investigations (Janarthanan et al., 2021). However, the distinctive features of these gadgets pose significant challenges for forensic analysis. Additional study is required to examine forensic techniques, tools, and methodologies that are specific to IoT devices in order to solve issues such as data extraction, analysis, and interpretation of sensor data, communication logs, and device configurations.

3 Materials and Methods

The Research Design

In this study, the researcher chose a mixed-methods research design that utilizes quantitative and qualitative information-gathering procedures to address the research questions and hypotheses. I chose three primary data collection strategies, i.e., observation, survey, and case study. In the quantitative approach, the researcher systematically gathered and examined data on challenges and techniques involved in forensic data analysis. Another quantitative data collection method, the survey questionnaire, was utilized to gather data from a larger sample size of forensic investigators and experts in the company we visited for the case study. This would allow for the systematic collection of structured data on the prevalence of specific challenges and the effectiveness of various strategies in counteracting certain obstacles in forensic analysis. Using this approach, the researcher planned to gain a statistics-based evaluation of different crucial aspects of security threats. The qualitative approach, on the other hand, entailed examining non-numerical data in an effort to comprehend user perspectives and experiences concerning emergent security challenges and risks (Sree & Bhanu, 2020).

Data Collection Methods and Procedures

Case Study: Two separate trips to various study locations that were carefully selected for the research were scheduled by the researcher. For the initial stage of data collecting for the case study, the researcher required a reliable cybersecurity firm with experience managing substantial volumes of digital data. I specifically required a company that handled digital forensic evidence for either private or public inquiries by government agencies. The researcher looked through publicly available records on digital forensic investigations over the previous five years on the internet before deciding on the best company. The researcher selected Security Bulls, a global cybersecurity company that offers scientific and technical know-how across a range of industries, including private investigation. According to online sources, it is one of the most trusted companies in cyber forensics, especially in its base country and largest market, China. The company management team assigned one of their cybersecurity experts to assist in studying two cases from their previous year's archives. The first case involved responding to a large-scale data breach at a major Beijing-based retail corporation in 2021.

Security Bulls' experts were engaged in responding to the breach and identifying the root cause of the security vulnerability the attackers had exploited. The company relied on mobile devices, such as mobile phones, tablets, and other gadgets provided by the affected company and the victim's family. These devices would help the experts assess the breach and provide the best security policies and procedures to prevent future attacks. The second case involved an expert response to a murder case of a senior manager of a company based in Hong Kong. Similarly, the affected company and family felt a significant loss. Therefore, they demanded accurate answers regarding the evidence from Security Bulls' cybersecurity experts in the quest to track and hold the perpetrators accountable for the loss. In this case, the investigators received all data records from the affected individual's storage systems. Using intrusion detection systems, they analyzed the devices and developed evidence of several steps that led to the crime. The researcher studied the two cases, noting similarities and differences in challenges and advancements, techniques, and abnormalities in the evidence extraction and analysis processes.

Observation: This data collection phase involved the researcher conducting a site visit to observe the actual process of retrieving and analyzing digital evidence from mobile devices. The observation aimed to examine the abnormalities surrounding these procedures. I reached out to Alura-link, one of the rapidly developing companies in cybersecurity and digital forensic investigation. I then established a set of plans to follow up with the analysis. Specifically, I focused on the advancement of mobile device forensic tools used in handling one of their numerous forensic investigation cases. During the procedure, digital evidence was collected and analyzed for a cybercrime investigation while the researcher recorded their findings. After collecting the needed data, the researcher analyzed it and compared the results with those obtained from the case study to determine the most efficient techniques for analyzing digital evidence in contexts sharing the same work environment. Throughout the process, the researcher adhered to all ethical considerations and ensured that all collected data were recorded and stored appropriately.

Survey Questionnaire for Security Bull’s Cyber Security Experts

Two of the cybersecurity specialists provided by the corporate management team helped to answer a prepared questionnaire after the observation and case study phases. The specialists at Security Bulls were working to contain different breaches at that time and determine what caused the security flaw that the attackers had taken on different clients. The business depended on mobile gadgets from the victim's family and the impacted organization, including tablets, smartphones, and other mobile devices. With the use of these tools, the professionals could evaluate the breach and provide the best security practices and guidelines to thwart similar incidents in the future. They offered their views regarding the prevalence of specific challenges and the effectiveness of various strategies in counteracting certain obstacles of forensic analysis, like the ones they were working on. The following are the survey questions administered to the security team.

1. What is your role and experience in digital forensic investigations at Security Bulls?
2. How frequently do you encounter challenges related to fragmented data during forensic analysis?
3. What are the most common sources of fragmented data that you encounter in your investigations?
4. How effective do you think current tools and techniques are in reconstructing fragmented data sets?
5. What are the main challenges you face in maintaining the integrity and authenticity of digital evidence during forensic analysis?
6. How do you address issues related to data encryption and password protection during forensic examinations?
7. In your experience, what are the key challenges associated with extracting data from mobile devices?
8. What strategies do you employ to overcome obstacles related to mobile device forensic analysis?
9. How prevalent are challenges related to cloud services in your forensic investigations?
10. What methods do you use to collect and analyze data stored in cloud environments?
11. How do you handle challenges related to jurisdictional issues and legal constraints in cross-border investigations?
12. What role does collaboration with law enforcement agencies play in overcoming challenges in forensic analysis?
13. How do you address challenges related to data tampering and anti-forensic techniques employed by perpetrators?

14. What strategies do you employ to mitigate risks associated with malware and malicious software during forensic examinations?
15. How do you stay updated on emerging threats and evolving techniques in forensic analysis?
16. Have you encountered challenges related to the proliferation of IoT devices in forensic investigations?
17. What strategies do you use to collect and analyze data from IoT devices securely?
18. How do you ensure compliance with relevant privacy laws and regulations during forensic examinations?
19. What are the main challenges you face in presenting forensic evidence in legal proceedings?
20. In your opinion, what areas require further research or improvement in the field of digital forensic analysis?

Materials and Primary Sources

There are numerous resources and primary sources that were suitable for my research in forensic analysis on mobile devices. For instance, academic publications and research articles are important sources because they provide in-depth analyses of the challenges, solutions, developments, and safety risks in mobile device forensic analysis. I chose mobile device forensics-specific books and textbooks that offered thorough information and theoretical foundations encompassing device-specific analysis techniques and legal considerations. Official documentation from device companies, operating system creators, and standards groups also provided reliable references for information on device specifications, storage architectures, encryption techniques, and forensic analysis best practices. The developer's documentation and user manuals for mobile device forensic tools made it easier to observe the compatibility of different kinds of phones with specific techniques.

Ethical Considerations

In this research involving non-participant data collection methods, i.e., case study and observation, confidentiality, institutional approval, respect for context and boundaries, data veracity, transparency, consent for publication, and the moral application of findings were the main ethical factors to consider in this research. The researcher achieved privacy and confidentiality by de-identifying and anonymizing sensitive information, securely storing data, and separating identifying information from study conclusions. I then requested the necessary authorization and approvals from the institutions in which I conducted my research. It is essential to respect the restrictions and boundaries set by the organizations or people involved and to ensure accurate and objective reporting of data. Therefore, I focused on maintaining the confidentiality of sensitive or confidential information while maintaining the transparency of reporting processes and conclusions. Additionally, the researcher handled all the procedures ethically while utilizing the results, preventing misuse, and encouraging responsible use for the advancement of the field while adhering to moral and legal requirements.

Data Analysis Techniques

The information analysis procedure for the study involved combining different findings from all the data collection methods involved in the mixed research. The quantitative data collected through observation were analyzed using statistical methods. The data were then categorized using quantitative methods. Descriptive statistics and inferential statistics were employed to observe trends and similarities. The researcher used thematic analysis techniques to examine the qualitative data gathered through the case study conducted. We thoroughly examined Security Bulls' cybersecurity specialists' survey questionnaire replies to find prevalent issues and useful tactics in their field. Quantitative information was utilized to measure the frequency of different challenges as well as the perceived efficacy of different approaches, as discussed below. The qualitative data of the open-ended questions were examined for recurrent themes using thematic analysis. We then organized the data into descriptive statistics and combined them with the data obtained from the other collection methods. Finally, textual data were categorized and analyzed to find important insights into the issue at hand.

Study Limitations

This study employed some of the most widely used data collection methods in scientific research. However, it has certain limitations that I should acknowledge. One disadvantage is the issue of generalizability. The fact that I used case studies and observation as the primary data collection techniques may be the source of bias that could render the results of this study not completely generalizable. The research may not have covered the whole range of mobile devices and forensic analysis techniques because it may have concentrated on selected devices, operating systems, or scenarios. Therefore, one needs more precaution when extending the results to various contexts or platforms. The accessibility of the data is another restriction. The availability of relevant information for analysis will determine how effective the study was. The availability and accessibility of some data sources may be constrained by elements like legal restraints or proprietary restrictions. As a result, the scope or depth of analysis in certain areas may be constrained. One should consider these limitations when interpreting and applying the findings of this study.

4 Results and Discussion

Summary of Findings

This section entails the key observations and in-depth analyses of the information gathered using the methods mentioned above. It highlights the quantitative and qualitative results while providing a space to delve into the ramifications of these findings for concerned authorities, stakeholders, and the general public. In my research, I undertook observation and case studies on two forensic analysis companies. I began the case study with Security Bulls and later went to the second forensic investigation company—Alura-link. In the first phase, the practice of forensic analysis of mobile devices in these organizations is shed light on. In this work, the most significant challenges faced by forensic investigators during mobile device analysis are discussed in detail. The most widespread were device heterogeneity and data fragmentation. The diversity of devices is also worth noting because it calls for a thorough knowledge of the distinctive qualities and complexities of each device, as well as the capacity to use device-specific analysis tools. Another issue is data fragmentation, which arises from the possibility that digital evidence may be dispersed over several storage mediums, including cloud services and interconnected IoT devices. Therefore, investigators need to create specific methods for retrieving and putting together dispersed data in order to create a reliable picture of the evidence. Its prevalent nature calls for investigators to traverse challenging access processes, verify data integrity, and resolve jurisdictional and privacy issues as a result of the increasing adoption of cloud storage and synchronization in almost all sectors.

Secondly, the study uncovered upcoming techniques and tools employed by investigators to overcome these challenges. Improved data extraction facilities, cloud data acquisition features, and advanced analysis apps, including social media analysis, were some of the new techniques preferred in the field by high-profile investigators. These would be crucial advancements in bringing the tools current with the current landscape of mobile devices and ensuring that device forensics would be continuous. Forensic investigators reconstructed deleted files or data pieces using data carving or file system analysis. Carving is the process of removing data (files) from undifferentiated chunks (raw data). File carving is the process of locating and restoring files using file format analysis. Carving is a useful method in Cyber Forensics to locate hidden or erased data from digital media. In this case, the investigators used these programs to examine the device's file system and locate deleted files that might still be present in fragmented clusters. From my observation, by separating and rebuilding these fragments, the investigators uncovered important evidence that would have otherwise been unreachable.

Security Bulls gave the researcher a chance to experience the challenges in this field first-hand, as they used a range of strategies, particularly file carving, to recover deleted or fragmented data and device exploitation to get around security measures in locked devices. When the most conventional methods of file recovery failed, data carving was usually employed even when files were corrupted, rewritten, or erased. Additionally, files from unused space or formatted drives were recovered using this method. The Security Bulls team also used cutting-edge mobile device forensic tools with improved data extraction capabilities in order to retrieve digital evidence from a range of devices and platforms. During the case study, I explored specific forensic analysis scenarios involving mobile devices at the second forensic investigation company. My findings illuminate the vitality of ensuring the integrity and admissibility of evidence by using careful data extraction and preservation strategies. The team gained access to cloud data and analyzed it even using APIs. They also made an attempt to recover data from damaged or encrypted databases, trying it with database reconstruction techniques. In other instances, it took cooperation with the judicial system to make the service providers produce the data. From my analysis, I was able to get another insight into how I was able to continue increasing mobile security threats. The problem of mobile malware seems to be growing and constitutes another serious challenge to forensic analysts. I must say that the second team in the forensic investigation company applied only the most progressive methods for the detection and analysis of malware and delivered a report listing the behavior of malicious applications, as suggested (Khan et al., 2020).

Interpretation

The examined companies showed good proficiency in managing the wide variety of mobile devices used in forensic investigation. They demonstrated proficiency in data extraction and analysis from a range of device models and software versions. As we know, we collect data from mobile devices using three methods: filesystem extraction, physical extraction, and logical extraction. Application Programming Interface (API) was used in the Logical Extraction, but the device's OS was not used in the File System Extraction or Physical Extraction processes. This is carried out right before the device's operating system kicks in. The phase is referred to as Bootloader. This interpretation is enough proof that investigators must keep up with the newest technology advancements and have an in-depth knowledge of distinctive features specific to each device. Advanced mobile device forensic technologies played a crucial role in recovering and analyzing digital evidence. The advanced data extraction capabilities offered by these tools enhanced effective, logical, physical, and file system extractions. Investigators were able to access relevant information stored in cloud services thanks to their connection with cloud data-acquiring features.

This clearly underscores the importance of mobile forensic investigators, or, for that matter, forensic investigators, being able to avail themselves of all the tools in an industry to be at their best. In use, such allowed the company to reassemble lots of fragmented data, for instance, by processes of file cutting and database reconstruction. It is, therefore, evident that there is a need for the use of specialized procedures that will help break data to enable the salvaging of important digital evidence. The study demonstrated the value of legal cooperation in acquiring the information required for forensic analysis. The organizations that I examined showed that they recognized and adhered to the procedures and legal frameworks necessary to access cloud-stored data and obtain service-provider collaboration. Additionally, they prioritized privacy concerns, ensuring that they handled delicate data safely and in accordance with privacy laws. This finding emphasizes the responsibilities that forensic investigators bear under the law and must be upheld in their practice.

Implications

The implications of the study conclusions and analysis towards future forensic investigation will help in the forensic investigation of mobile device forensic analysis methods and improvements. This will inform the investigator of the strategies, tools, and methodologies that need to be used and the challenges that need to be overcome. These may lead to improvements in the efficiency and precision of the forensic analysis methods, and hopefully, these should ultimately improve the investigation outcomes. They will also have implications for the improvement of forensic methods and instruments.

It tells the tool developers, forensic laboratories, and investigators about every improvement and update required in light of the changing mobile device landscape and security threats. The above would promote inventiveness and better, effectual structures to aid in the gathering and analysis of digital evidence recovered from mobile devices. The study also emphasizes how training and skill advancement in the area of mobile device analysis are affected. The strategies and challenges that have been found highlight the necessity for researchers to keep up-to-date on their knowledge and abilities in order to stay on top of a developing field.

5 Conclusion

It is notable that this study focused on some other important aspects that will be helpful for further improvements in forensic tools and techniques, training, and skills development. This study discussed the most common problems that forensic investigators face. Therefore, the results from this research would demonstrate that during the collection and analysis of digital evidence from mobile devices, techniques used include device exploitation, password cracking, file carving, and database reconstruction. These findings have important effects on the development of mobile device forensic technologies, including improved data extraction skills, cloud data collecting, and advanced app analysis. Particularly, improvements in data collection will improve things like scalability. Businesses can scale analytics on the cloud to save money on on-premises data storage. You can increase data analysis and storage capacity by utilizing cloud computing as needed to accommodate organizational changes. Also, forensic analysts can now access critical evidence from mobile devices and traverse their complexity. The research results offer useful recommendations for enhancing investigation procedures, advancing forensic technologies, encouraging ongoing training and skill development, and assuring compliance with legal and ethical requirements in mobile device forensic analysis.

Directions for Future Research

Several future research opportunities can be identified based on the results and implications of this paper. First, there needs to be standardization and the creation of best practices for the forensic investigation of mobile devices. Future research could focus on the development of standardized protocols and recommendations for data extraction and evidence preservation. There is a pressing need for evidence integrity. The secret to solving every crime is the evidence. For evidence to be admitted in a court of law, its integrity must be maintained. Although digital evidence is more transparent, it is brittle and readily altered. Various methods exist for safeguarding the authenticity of digital evidence. However, it would be even better to improve this field through continued and focused research. Such initiatives would encourage reliability and consistency across investigations, hence raising the standard of forensic analysis in the field. Additionally, more studies are necessary in the field of IoT device forensics to understand the particular difficulties posed by connected IoT devices. This focus is specifically essential as the number of these devices continues to rise in the modern interconnected world. Future research can also look into the development of specialized tools and techniques designed specifically for the forensic examination of IoT devices. IoT devices often utilize 5G connectivity, which is currently one of the fastest forms of communication. The fast connectivity opens new windows for malicious actors to exploit. Therefore, more research is needed to expand the knowledge in this field. Data extraction and analysis require more advanced tools or a mix of computer forensic and network forensic tools and techniques. Extensive reverse engineering methods might be needed to retrieve data kept in particular proprietary formats. Since a successful cyberattack on an IoT device can seriously harm an organization's reputation, IoT security monitoring and extensive knowledge of this concept help guarantee that these assets are shielded from cyberattacks and data breaches. Part of this research will address the complexity caused by various communication protocols, exclusive operating systems, and IoT device-specific data storage techniques.

References

[1] Abdulaziz, N., Amin, S., & Bilal, M. (2023). Analog to digital converter: Novel Methodology. *International Journal of Communication and Computer Technologies (IJCCTS), 11*(2), 33-41.

[2] Abinaya, R., Vidhya, S., & Vadivel, S. (2014). Latent Palm Print Matching Based on Minutiae Features for Forensic Applications. *International Journal of Communication and Computer Technologies (IJCCTS)*, *2*(2), 85-87.

[3] Afzal, B., Umair, M., Shah, G.A., & Ahmed, E. (2019). Enabling IoT platforms for social IoT applications: Vision, feature mapping, and challenges. *Future Generation Computer Systems, 92*, 718-731.

[4] Al-Dhaqm, A., Abd Razak, S., Ikuesan, R.A., Kebande, V.R., & Siddique, K. (2020). A review of mobile forensic investigation process models. *IEEE access, 8,* 173359-173375.

[5] Aljahdali, A., Alsaidi, N., Alsafri, M., Alsulami, A., & Almutairi, T. (2021). Mobile device forensics. *Romanian Journal of Information Technology & Automatic Control*, *31*(3), 81-96.

[6] Al-Turjman, F., & Salama, R. (2021). Cyber security in mobile social networks. *In Security in IoT Social Networks*, 55-81.

[7] Atlam, H.F., Hemdan, E.E.D., Alenezi, A., Alassafi, M.O., & Wills, G.B. (2020). Internet of things forensics: A review. *Internet of Things, 11*, 100220. https://doi.org/10.1016/j.iot.2020.100220

[8] Azad, P., Navimipour, N.J., Rahmani, A.M., & Sharifi, A. (2020). The role of structured and unstructured data managing mechanisms in the Internet of things. *Cluster computing*, *23,* 1185-1198.

[9] Bouchaud, F., Vantroys, T., & Grimaud, G. (2021). Evidence gathering in IoT criminal investigation. *In Digital Forensics and Cyber Crime: 11th EAI International Conference, ICDF2C 2020, Boston, MA, USA, October 15-16, 2020, Proceedings,* 44-61.

[10] Cantrell, G. (2019). Teaching data carving using the real-world problem of text message extraction from unstructured mobile device data dumps. *Journal of Digital Forensics, Security & Law*, *14*(4).

[11] Casey, E. (2019). The chequered past and risky future of digital forensics. *Australian journal of forensic* sciences, *51*(6), 649-664.

[12] Casino, F., Dasaklis, T.K., Spathoulas, G.P., Anagnostopoulos, M., Ghosal, A., Borocz, I., & Patsakis, C. (2022). Research trends, challenges, and emerging topics in digital forensics: A review of reviews. *IEEE Access*, *10*, 25464-25493.

[13] Connolly, L.Y., & Wall, D.S. (2019). The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures. *Computers & Security*, *87*, 101568. https://doi.org/10.1016/j.cose.2019.101568

[14] Da Silveira, C.M., De Oliveira Albuquerque, R., Amvame Nze, G.D., De Oliveira Júnior, G.A., Sandoval Orozco, A.L., & García Villalba, L.J. (2020). Methodology for forensics data reconstruction on mobile devices with Android operating system applying in-system programming and combination firmware. *Applied Sciences*, *10*(12), 4231. https://doi.org/10.3390/app10124231.

[15] Ertam, F., Yakut, O.F., & Tuncer, T. (2023). Pattern lock screen detection method based on lightweight deep feature extraction. *Neural Computing and Applications, 35*(2), 1549-1567.

[16] Ferguson, R.I., Renaud, K., Wilford, S., & Irons, A. (2020). PRECEPT: a framework for ethical digital forensics investigations. *Journal of Intellectual Capital, 21*(2), 257–290.

[17] 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. https://doi.org/10.1016/j.fsidi.2021.301169

[18] Groß, T. H. (2022). *Forensic Data Extraction from Modern File Systems* (Doctoral dissertation, Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU)). https://open.fau.de/handle/openfau/19691.

[19] Harkin, D., Molnar, A., & Vowles, E. (2020). The commodification of mobile phone surveillance: An analysis of the consumer spyware industry. *Crime, media, culture, 16*(1), 33–60.

[20] Hou, S., Sasaki, R., Uehara, T., & Yiu, S.M. (2013). Double Encryption for Data Authenticity and Integrity in Privacy-preserving Confidential Forensic Investigation. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 4*(2), 104-113.

[21] Janarthanan, T., Bagheri, M., & Zargari, S. (2021). IoT forensics: an overview of the current issues and challenges. *Digital Forensic Investigation of Internet of Things (IoT) Devices*, 223-254.

[22] Jelena, T., & Srđan, K. (2023). Smart Mining: Joint Model for Parametrization of Coal Excavation Process Based on Artificial Neural Networks. *Arhiv za tehničke nauke*, *2*(29), 11-22.

[23] Khan, W.Z., Rehman, M.H., Zangoti, H.M., Afzal, M.K., Armi, N., & Salah, K. (2020). Industrial internet of things: Recent advances, enabling technologies and open challenges. *Computers & electrical engineering*, *81*, 106522. https://doi.org/10.1016/j.compeleceng.2019.106522.

[24] Lee, Y., & Woo, S. (2022). Practical Data Acquisition and Analysis Method for Automobile Event Data Recorders Forensics. *Journal of Internet Services and Information Security*, *12*(3), 76-86.

[25] Lim, K.W., Kapusta, K., Memmi, G., & Jung, W.S. (2019). Multi-hop Data Fragmentation in Unattended Wireless Sensor Networks. *arXiv preprint arXiv:1901.05831*.

[26] Marques, D., Guerreiro, T., Carriço, L., Beschastnikh, I., & Beznosov, K. (2019). Vulnerability & blame: Making sense of unauthorized access to smartphones. *In Proceedings of the chi conference on human factors in computing systems*, 1-13.

[27] Miloslavskaya, N., & Tolstoy, A. (2019). Internet of Things: information security challenges and solutions. *Cluster Computing*, *22*, 103-119.

[28] Muralidharan, J. (2020). Wideband Patch Antenna for Military Applications. *National Journal of Antennas and Propagation (NJAP)*, *2*(1), 25-30.

[29] Pakkiraiah, C., & Satyanarayana, R.V.S. (2024). Design and FPGA Realization of Energy Efficient Reversible Full Adder for Digital Computing Applications. *Journal of VLSI Circuits and Systems, 6*(1), 7-18.

[30] Ram, A., & Chakraborty, S. K. (2024). Analysis of Software-Defined Networking (SDN) Performance in Wired and Wireless Networks Across Various Topologies, Including Single, Linear, and Tree Structures. *Indian Journal of Information Sources and Services, 14*(1), 39–50.

[31] Roumani, Y. (2022). Detection time of data breaches. *Computers & Security*, *112*, 102508. https://doi.org/10.1016/j.cose.2021.102508.

[32] Rudie, J.D., Katz, Z., Kuhbander, S., & Bhunia, S. (2021). Technical analysis of the NSO group's Pegasus spyware. *In International Conference on Computational Science and Computational Intelligence (CSCI)*, 747-752.

[33] Ryu, J.H., Sharma, P.K., Jo, J.H., & Park, J.H. (2019). A blockchain-based decentralized efficient investigation framework for IoT digital forensics. *The Journal of Supercomputing*, *75*, 4372–4387.

[34] Sayakkara, A., Le-Khac, N. A., & Scanlon, M. (2019). A survey of electromagnetic side-channel attacks and discussion on their case-progressing potential for digital forensics. *Digital Investigation*, *29*, 43-54.

[35] Siriwardhana, Y., Porambage, P., Liyanage, M., & Ylianttila, M. (2021). AI and 6G Security: Opportunities and challenges. *In Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit*, 616-621.

[36] Sree, T.R., & Bhanu, S.M.S. (2020). Data collection techniques for forensic investigation in the cloud. *Digital Forensic Science*, 101-157.

[37] Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., & Markakis, E.K. (2020). A survey on the Internet of Things (IoT) forensics: challenges, approaches, and open issues. *IEEE Communications Surveys & Tutorials*, *22*(2), 1191-1221.

[38] Sumithra, S., & Sakshi, S. (2024). Exploring the Factors Influencing Usage Behavior of the Digital Library Remote Access (DLRA) Facility in a Private Higher Education Institution in India. *Indian Journal of Information Sources and Services, 14*(1), 78–84.

[39] Sunde, N., & Dror, I.E. (2019). Cognitive and human factors in digital forensics: Problems, challenges, and the way forward. *Digital investigation, 29*, 101-108.

[40] Wright, M. K. (2019). Financing Cr-ISIS: the efficacy of mutual legal assistance treaties in the context of money laundering and terror finance. *Vand. J. Transnat'l L., 52*, 229.

Author Biography

Bandr Fakiha Associate Professor at the Department of Medical Health Services, Dean of Faculty of Health Sciences, Umm Al-Qura University. Al Qunfudh. Saudi Arabia. His research interests include cyber forensics, cybersecurity, computer forensics, forensic information technology, and digital forensics.