Addressing the Hurdles in Mobile Forensic Investigations

Vedant Marwadi - 23208466

Digital Forensics Tools and Techniques, Master of Computer and Information Sciences,
Auckland University of Technology

Contents

Software Used

1. Overleaf: for writing and compiling the report.
2. Zotero: for managing references.
3. Grammarly: for checking and correcting grammar and sentence structure.

1. Introduction

Mobile devices have become indispensable in daily life. They provide uninterrupted access to information and serve as a primary tool for communication in the digital world (Chernyshev et al., 2017). As a result, they have evolved to possess substantial storage capacities and powerful processing capabilities, which allow them to hold vast amounts of personal and organizational information (Bennett, 2012).

However, with the increasing incorporation of smartphones into personal habits, their involvement in criminal activities is also becoming more prevalent (Yadav et al., 2013). Nearly every type of crime these days involves some form of digital evidence found on mobile phones (Bennett, 2012). This growing trend has prompted the establishment of mobile forensics as a specialized field within digital forensics (Barmpatsalou et al., 2019).

Mobile forensics is described as the discipline of extracting digital evidence from mobile devices in a forensically sound manner utilizing recognized techniques (Zareen & Baig, 2010). This field is essential because mobile devices contain a vast amount of data that can be vital to both civil and criminal investigations (Kumar, 2021).

Despite its importance, mobile forensics presents unique challenges to investigators. These complexities often impact both the efficiency and effectiveness of forensic investigations (Umale et al., 2014). This report delves into these difficulties, with an emphasis on device diversity, tool limitations, data volatility, cloud integration, security mechanisms, and legal considerations. By highlighting these multifaceted issues, the report aims to draw attention to the obstacles faced by investigators in mobile forensics.

2. Discussion

Law enforcement, intelligence agencies, and private investigators are increasingly relying on mobiles to gather evidence (Lutes & Mislan, 2008). These devices have a high potential for holding digital evidence that can be crucial in criminal investigations (Zareen & Baig, 2010). However, due to their inherent design and functionality mobile forensics presents complex difficulties (Kumar, 2021). These challenges include:

2.1 Device Diversity:

The accelerated growth and variety of mobile devices present significant challenges for forensic investigators. The current market is flooded with numerous cell phone manufacturers, each producing multiple models with unique features and data storage structures (Khubrani, 2023). This constant evolution makes it difficult for forensic tools and methods to keep up with the latest advancements (Bennett, 2012). Consequently, forensic

investigators must continually update their methods to keep pace with the rapid evolution of mobile devices and ensure reliable data retrieval.

Additionally, these smartphones operate on various operating systems, primarily iOS and Android, but also others like BlackBerry (Bennett, 2012). Frequent updates to these operating systems introduce new features and security measures, which complicate forensic investigations (Yadav et al., 2013). As a result, to effectively extract data, forensic experts must maintain expertise in the diverse platforms and remain current with their ongoing changes(Khubrani, 2023).

Furthermore, each operating system has its own file systems, security features, and data storage methods (Raghav & Saxena, 2009). Even within a single OS, there are numerous versions. For example, iOS has over 40 versions spread across different models of iPhones, iPads, and iPods. On the other hand, Android devices are particularly challenging because users rarely upgrade their OS, leading to a vast array of versions in use simultaneously (Umale et al., 2014). The presence of illegally modified or counterfeit operating systems further complicates the forensic process (Yadav et al., 2013). Thus, the diverse and evolving nature of operating systems adds another layer of difficulty for forensic investigators striving for accurate and reliable data analysis.

2.2 Tool Limitations:

There is no single forensic tool that supports all makes and models of mobile phones. The lack of universal tools means that investigators often need to use multiple tools to handle different devices (Umar et al., 2018). However, most international training programs are vendor-specific, which sometimes limits the ability of examiners to work with tools from other vendors (Zareen & Baig, 2010). This demands continuous training for investigators. Without appropriate knowledge, expertise, and practice, forensic investigators risk making critical errors that might lead to the loss of crucial data (Bajramovid, 2014).

Conversely, it should be noted that forensic tools may also inadvertently modify data, compromising the integrity of the evidence (Kumar, 2021). Most commercially available forensic tools are not equipped to handle physically damaged phones (Zareen & Baig, 2010). Not to mention, forensic tools are also susceptible to software bugs and vulnerabilities. This compromises their dependability and forensic integrity. Moreover, various forensic tools might generate differing outcomes when extracting evidence under similar conditions, which creates challenges in determining admissible evidence. (Chernyshev et al., 2017).

Many mobile operating systems are proprietary and closed source, making it difficult to develop and test forensic tools. The short release cycles of mobile operating systems, with

new versions being released frequently, exacerbate this issue. This rapid development pace makes it challenging for forensic tools to keep up, leading to delays in supporting the latest devices (Ahmed & Dharaskar, 2008).

Lastly, the combination of mobile devices with IoT services has broadened the range of digital investigations. This expansion includes new device categories such as smartwatches, which require the creation and validation of new tools and methods for evidence extraction and analysis (Chernyshev et al., 2017). However, the high cost of forensic tools and budget constraints may limit the availability of the latest tools and technology needed to address these new complications (Yadav et al., 2013).

2.3 Data Volatility:

It is a fundamental principle in digital forensics to guarantee that evidence is not destroyed or altered during the extraction and analysis process (Kumar, 2021). This is particularly challenging with mobile devices because, unlike computers that typically use nonvolatile hard disk drives, smartphones use volatile memory, resulting in potential data loss if the device loses power. Similarly, the dynamic nature of mobile phones, which constantly updates information in their memory, adds further complexity. This makes it challenging to create a bitwise copy of all data stored in mobile phones, which is a standard procedure in traditional computer forensics. The inability to create a consistent forensic hash value for mobile phone memory complicates the verification of evidence integrity (Ahmed & Dharaskar, 2008).

Additionally, mobile phones do not have conventional write-blocking mechanisms like traditional storage media, meaning data can change during analysis. For instance, opening unread messages or emails can change their status, potentially altering the evidence (Zareen & Baig, 2010). Browsing an app can modify its data, and updates or modifications to the device's operating system can alter data structures and storage methods, further complicating forensic analysis (Sharma et al., 2021). Even changing power modes can modify critical information and might even trigger malicious code designed to destroy data (Yadav et al., 2013). To make matters worse, most mobile phones have a factory reset option that erases all data and restores the device to its original settings. If this is done before or during forensic analysis, it can result in the loss of crucial evidence (Kumar, 2021).

2.4 Cloud Integration:

Mobile devices hold data in multiple places, such as internal memory, external memory cards, and app-specific storage, complicating the task of accurately recreating user activities. (Khubrani, 2023). This issue is exacerbated by the increasing synchronization of data

with cloud services, resulting in a substantial portion of user data being stored remotely rather than on the device itself (Raghav & Saxena, 2009).

The nature of mobile cloud computing involves data being distributed across various virtual environments, making it difficult for investigators to track and identify specific data. Compounding this issue is the fact that investigators often lack access to the physical resources where data is stored because these resources are managed by Cloud Service Providers. Digital investigators need permission from CSPs to access data, which often requires legal documentation. The complexity increases when data spans multiple data centers, possibly located in different geographical regions (Khan et al., 2014). Beyond that, ensuring user privacy adds an additional layer of difficulty in pinpointing evidence among numerous virtual components (Chernyshev et al., 2017).

Adding to this complexity, logs and data records are often stored across various data centers in different time zones, leading to time synchronization issues. This can complicate the reconstruction of events. When presenting evidence in court, the lack of synchronized timestamps can create difficulties in proving the sequence and integrity of events (Khan et al., 2014).

2.5 Security Mechanisms:

Modern mobile devices employ various locking mechanisms to safeguard user data. While these measures effectively protect user information, they also present considerable impediments for investigators attempting to access potential evidence (Barmpatsalou et al., 2019; Khubrani, 2023). Advanced biometric unlock schemes, such as face unlocking technology and fingerprint scanners, can be accidentally triggered, costing forensic specialists one chance at unlocking the device. This especially is concerning because even budget devices in today's market come equipped with such biometric features (Herrera, 2020).

Although tools exist to bypass these security measures, they are not always effective for all devices and OS versions (Kumar, 2021). Besides, some devices are programmed to automatically delete data after multiple failed access attempts, thereby leading to the loss of critical evidence (Barmpatsalou et al., 2019). Without the correct unlock code or biometric input, retrieving the data stored on the device becomes a big problem for forensic investigators (Raghav & Saxena, 2009).

2.6 Legal Considerations:

Mobile devices store highly sensitive personal information, such as private communications, financial data, and personal photos. Therefore, investigators must handle this data with care, respecting privacy rights and adhering to legal standards. Particularly, the

Fourth Amendment protects against unreasonable searches and seizures, which means investigators must obtain proper warrants before accessing digital data on smartphones. Thus, achieving a balance between protecting individual privacy and fulfilling the needs of an investigation makes a task more complex (Khubrani, 2023). The necessity to maintain this balance can also lead to delays in investigations (Bennett, 2012).

Furthermore, mobile phone investigations often span multiple jurisdictions and legal systems, necessitating forensic examiners to be knowledgeable about international laws and regulations. Different jurisdictions have varying laws regarding data privacy and the admissibility of digital evidence (Sharma et al., 2021). Legal constraints can impede evidence collection and analysis, especially when dealing with multinational companies and varying privacy laws (Kumar, 2021).

3. Conclusion

Based on these studies, it can be concluded that although mobile forensics plays a crucial role in law enforcement, it faces numerous challenges. It is observed that at the core of these issues is the evolving landscape of mobile technology. The proprietary nature of many mobile operating systems, coupled with their short release cycles, renders the forensic tools and methodologies ineffective.

Further complicating the problem is the volatile nature of mobile device memory, creating a real risk of losing crucial evidence. It is also noted that, the increasing synchronization of smartphones with cloud services disperses data across multiple virtual environments. This dispersion makes it challenging to reconstruct a complete user activity history without navigating the legal and logistical hurdles of accessing cloud-stored data.

Additionally, it is recognized that modern smartphones are equipped with robust security mechanisms, which provide strong user data protection, but also present critical barriers for forensic investigators. Legal considerations add yet another layer of complexity to mobile forensics. The need to carefully balance privacy rights with investigative requirements hampers the timely and effective collection of digital evidence.

To address these challenges, a multifaceted approach is required. The complexities inherent in mobile forensics cannot be resolved through a single solution but rather through a combination of technological, educational, legal, and collaborative efforts. Future research should focus on the standardization of procedures and tools in mobile forensics. This would help create a uniform approach, reduce the variability currently impeding the field, and enhance the reliability of forensic findings. By overcoming these challenges, mobile forensics can remain vital for digital investigations, cybersecurity, and the pursuit

of justice in the digital age.

References

Ahmed, R., & Dharaskar, R. V. (2008). Mobile Forensics: An Overview, Tools, Future trends and Challenges from Law Enforcement perspective.

Bajramovid, E. (2014). CHALLENGES IN MOBILE FORENSICS TECHNOLOGY, METHODOLOGY, TRAINING, AND EXPENSE.

Barmpatsalou, K., Cruz, T., Monteiro, E., & Simoes, P. (2019). Current and Future Trends in Mobile Device Forensics: A Survey. *ACM Computing Surveys*, 51(3), 1–31. https://doi.org/10.1145/3177847

Bennett, D. (2012). The Challenges Facing Computer Forensics Investigators in Obtaining Information from Mobile Devices for Use in Criminal Investigations. *Information Security Journal: A Global Perspective*, 21(3), 159–168. https://doi.org/10.1080/19393555.2011.654317

Chernyshev, M., Zeadally, S., Baig, Z., & Woodward, A. (2017). Mobile Forensics: Advances, Challenges, and Research Opportunities. *IEEE Security & Privacy*, 15(6), 42–51. https://doi.org/10.1109/MSP.2017.4251107

Herrera, L. A. (2020). Challenges of acquiring mobile devices while minimizing the loss of usable forensics data. *2020 8th International Symposium on Digital Forensics and Security (ISDFS)*, 1–5. https://doi.org/10.1109/ISDFS49300.2020.9116458

Khan, S., Ahmad, E., Shiraz, M., Gani, A., Wahab, A. W. A., & Bagiwa, M. A. (2014). Forensic challenges in mobile cloud computing. *2014 International Conference on Computer, Communications, and Control Technology (I4CT)*, 343–347. https://doi.org/10.1109/I4CT.2014.6914202

Khubrani, M. M. (2023). Mobile Device Forensics, challenges and Blockchain-based Solution. *2023 Second International Conference On Smart Technologies For Smart Nation (SmartTechCon)*, 1504–1509. https://doi.org/10.1109/SmartTechCon57526.2023.10391719

Kumar, M. (2021). Mobile phone forensics - a systematic approach, tools, techniques and challenges. *International Journal of Electronic Security and Digital Forensics*, 13(1), 64. https://doi.org/10.1504/IJESDF.2021.111725

Lutes, K. D., & Mislan, R. P. (2008). Challenges in Mobile Phone Forensics.

Raghav, S., & Saxena, A. K. (2009). Mobile forensics: Guidelines and challenges in data preservation and acquisition. *2009 IEEE Student Conference on Research and Development (SCOReD)*, 5–8. https://doi.org/10.1109/SCORED.2009.5443431

Sharma, B. K., Yadav, V., Purba, M. K., Sharma, Y., & Mehta, P. (2021). Challenges, Tools, and Future of Mobile Phone Forensics.

Umale, M. M. N., Deshmukh, A., & Tambhakhe, M. (2014). Mobile phone forensics challenges and tools classification: A review. *International Journal on Recent and Innovation Trends in Computing and Communication*, 2(3), 622–626.

Umar, R., Riadi, I., & Zamroni, G. M. (2018). Mobile Forensic Tools Evaluation for Digital Crime Investigation. *International Journal on Advanced Science, Engineering and Information Technology*, 8(3), 949. https://doi.org/10.18517/ijaseit.8.3.3591

Yadav, D., Mishra, M., & Prakash, S. (2013). Mobile Forensics Challenges and Admissibility of Electronic Evidences in India. *2013 5th International Conference on Computational Intelligence and Communication Networks*, 237–242. https://doi.org/10.1109/CICN.2013.57

Zareen, A., & Baig, S. (2010). Notice of Violation of IEEE Publication Principles: Mobile Phone Forensics: Challenges, Analysis and Tools Classification. *2010 Fifth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering*, 47–55. https://doi.org/10.1109/SADFE.2010.24