Using Digital Forensics for Android Smartphone Devices to aid Criminal Investigations

Stephanie Agenbag[1], Andre Henney[1] and Heloise Pieterse[2]
[1]Department of Computer Science, Faculty of Natural Science, University of the Western Cape, Bellville, South Africa
[2]Council for Scientific and Industrial Research, Pretoria, South Africa

3844494@myuwc.ac.za
ahenney@uwc.ac.za
hpieterse@csir.co.za

Abstract: In the past decade, there has been an exponential adoption and ownership of smartphones by billions of users worldwide. However, as smartphone usage increases, criminals have taken advantage of them for illicit or criminal purposes. In criminal investigations, smartphone data has become an invaluable source of information. This study focuses on constructing a snapshot of Android-operated smartphone data to assist investigators in answering critical investigative questions. A thorough review of the literature with regard to the use of smartphone evidence in criminal cases, with the goal of emphasising the investigative phase and the supportive role of mobile data evidence in guiding investigations will be performed. In order to identify additional persons of interest and develop a thorough understanding of the case, the methodology will entail analysing user profiles, smartphone usage patterns, communication logs, application usage, geographic lookups, and device interactions. By conducting a thorough examination of relevant literature, designing a suitable model, and executing a case study, the study intends to offer valuable perspectives on the creation of timelines or visual representations derived from smartphone data. The results of this study will contribute to improving the efficacy of mobile forensics in assisting investigators and facilitating the use of Android-operated smartphone data as supporting evidence in criminal investigations.

Keywords: Digital Forensics, Mobile Forensics, Android-Smartphones, Digital Evidence, Data Analysis

1. Introduction and Background

Smartphones were introduced to the general public over a decade ago. Since their release, they have become increasingly popular over the years as technology evolved. By the end of 2022, there were nearly 6.6 billion smartphone users across the globe (Taylor, 2023). The average smartphone is now a camera, music player, GPS, and telephonic device, all in one. As smartphones have become more popular, they have also become more affordable, making them accessible to a wider range of people.

Smartphones have become an integral part of modern life, but unfortunately, they are also being misused by criminals for various illegal activities. In 2015, Anwar Fisher was convicted of statutory rape and sexual assault based on text messages and inappropriate photos discovered by the victim's mother, resulting in a 2018 confirmation of his six-count conviction (Fisher v S (A51/2016), 2018).

One domain that is largely overlooked is that of criminal investigations, where smartphones have emerged as valuable sources of potential evidence. Acknowledging the strong link between smartphone usage and its relevance in criminal cases, researchers McMillan, Glisson and Bromby (2013) and Zhang et al. (2022) embarked on empirical studies to establish and support this idea. Their findings have inspired the research direction of this study.

In cases where smartphones are seized as evidence, reconstructing their data can be a valuable technique for aiding an investigation. This will give the investigators a method of visualising a timeline of occurrences or a timeline of user activities leading up to an incident. This study will exclusively focus on the Android operating system given Android's dominant global market share of 70.5% in the third quarter of 2023 (Statista Research Department, 2023).

2. Problem Statement

The proposed research will focus on constructing a snapshot of the data retrieved from a smartphone linked to an investigation to assist the investigator. Therefore, the main focus is on the extraction of relevant information from the rich data sources on a smartphone. The goal is to leverage the extracted information to answer critical investigative questions such as who, what, where, when, how, and why certain criminal activities occurred. This information is crucial for building a comprehensive understanding of the activities that

took place on a smartphone. As a result, an overview, either in the form of a timeline or a visual reference, of the user's activities on the smartphone leading up to and during the incident under investigation.

The research question:

How to construct a snapshot of smartphone data to assist a criminal investigation?

3. Literature Review

While the broader field of digital forensics has undergone extensive research, the subdomain of mobile forensics remains in its early stages, marked by a conspicuous scarcity of literature dedicated specifically to mobile forensic investigations. Papers that focused on reviewing mobile forensics in the realm of digital forensics, such as those authored by Dogan and Akbal (2017), and Alatawi et al. (2020), provided a comprehensive overview of the Digital forensic process. This process encompasses four main phases: collection, examination, analysis, and reporting. Additionally, these papers discussed various acquisition methods and tools designed to facilitate the analysis of potential data.

3.1 The Prominence of Mobile Forensics in Criminal Court

McMillan, Glisson and Bromby (2013) took note of the ever-growing popularity of mobile phones and how this could lead to an increase in potential evidence sources in criminal cases. While this correlation appears to be unambiguous, the authors required empirical evidence to substantiate this notion. The study covered cases from 2006 to 2011, obtained through database searches using keywords. Relevant cases were manually selected, and their information extracted into a Microsoft Access database. The analysis of appeal judgments confirms that mobile phone evidence in criminal court cases has been on the rise, showing a correlation between evidence type and the nature of the crimes investigated.

Another Chinese study, drawing inspiration from previous research, investigated various aspects of mobile phone evidence in criminal proceedings from 2013 to 2018. The study focused on determining the proportion of cases that employ mobile phone evidence, examining the types of crimes and mobile phone data involved, exploring the connection between different types of evidence and specific criminal proceedings, and evaluating the significance of mobile phone evidence in court proceedings (Zhang et al., 2022). The study revealed that mobile phone evidence was utilised in a small proportion of the cases included in the dataset, but there was a slight upward trend in the usage of mobile phone evidence over the years.

Despite these papers differing in terms of geographical focus, time period, data sources, and methodologies, they produced very similar results. These papers conclude that it seems like a large amount of mobile phone evidence is filtered out in the stages before court proceedings. Both studies have suggested that future research should focus on exploring the use of mobile data evidence during the investigatory phase rather than solely emphasising its role in court proceedings.

The use of smartphone data as court evidence is a complex and multifaceted subject, with ongoing discussions surrounding the forensic soundness of the techniques and tools employed. However, the aforementioned studies reaffirm the importance of accessing and effectively utilising this data during the investigative process, thereby corroborating the original research direction.

3.2 Extracting and Analysing Smartphone Data

The authors of the paper titled “Mobile Device Forensics: Extracting and Analysing Data from an Android-Based Smartphone” experimented with various methods of extracting and analysing data from Android smartphones using the Sleuth Kit Autopsy (Aziz, Mokhti and Nozri, 2016). The paper begins by highlighting the ubiquity of mobile devices, particularly smartphones, and their increasing use in criminal activities.

The methodology outlines the computer forensic process for Android smartphones, addressing challenges stemming from the diversity of smartphone manufacturers and iterations. The authors utilise the Sleuth Kit Autopsy tool to create a forensic image of the smartphone's data partition. A case study illustrates this approach in a corporate crime investigation, showcasing successful decryption of encrypted messages during the findings and analysis.

In their respective case studies, Jones and Winster (2017) employed Oxygen Forensics, a commercial forensic tool, while Al-Hadadi and AlShidhani (2013) utilised Oxygen Forensics along with UFED Physical Analyzer Cellebrite, mirroring the approach taken in the study conducted by Aziz, Mokhti, and Nozri (2015). Although the depth of analysis in these studies exceeded the capabilities provided by the freeware, the research

conducted by Aziz, Mokhti, and Nozri (2015) shows that retrieving fundamental information and gathering essential data for investigating their case study is achievable. Their paper could have benefited from exploring the case study using both commercial and freeware tools to facilitate result comparisons.

3.3 Exploring Potential Sources of Evidence in Smartphone Data

The research paper titled "Mobile Forensics: Beyond Traditional Sources of Digital Evidence" explores the importance of contemporary sources of data on mobile devices for digital forensic investigations (Pieterse, 2020). Traditionally, digital forensic investigations have focused on data such as contacts, messages, call history, and web browsing. However, this paper highlights the often-overlooked sources of data, including log files, usage statistics, and event data. The paper presents the Pre-Analysed Device Snapshot (PADS) model for creating a snapshot of a mobile device's state at the time of acquisition using contemporary data sources. It was practically evaluated with data from a Samsung Galaxy S5 Mini running Android 6.0.1, successfully identifying the user profile, recent app usage, and other activities on the device.

In principle, expanding the scope of what we can investigate offers investigators access to a multitude of potential data. However, the practicality of this approach is hindered by the substantial increase in the storage capacity of smartphones and the typically high number of installed apps. The enormous time, financial, and resource commitment that such a thorough investigation could require is the cause of this formidable challenge. This is not addressed in the paper would necessitate investigation if the model or any derivative form of inspiration were to be incorporated into the proposed study.

4. Research Framework

A qualitative research approach will be used to delve into the complex interactions and behaviours within smartphone data during criminal investigations. This method provides in-depth insights into the experiences, perspectives, and contextual details of individuals involved.

The study will employ an in-depth literature review, which will specifically focus on the following: (1) available smartphone data and (2) acquisition methods to extract the data from the smartphones. The objective is to develop a thorough understanding of the most advanced techniques and data sources that are currently available for smartphone data.

Thereafter, based on the extracted features, a model will be developed to construct a snapshot of the smartphone data. The model will accept as input the smartphone data and as output produce the timeline or visual reference that presents the user's activities leading up to and during the incident.

Finally, the model's evaluation will involve a case study focusing on specific criminal investigations, which may use either simulated or real-world smartphone data. If acquiring real-world smartphone data is not feasible, the authors will simulate data sources based on various smartphone usage scenarios. Subject to ethical and legal considerations, this can be obtained from sources like law enforcement authorities. Ethical considerations and data protection will be crucial if the case study uses real-world data.

The results will be addressed in relation to the research question and aims, with a focus on how investigators using smartphone data in criminal cases can use them in real-world situations. The research framework outlined above will form the groundwork of the proposed study that will provide valuable insights into generating timelines from smartphone data, contributing to the existing knowledge in this domain.

5. Contribution and Conclusion

The motivation for the proposed study stems from the conclusions drawn in the studies by McMillan, Glisson and Bromby (2013) and Zhang et al. (2022). The findings of both studies indicate that rather than solely emphasising its role in court proceedings, future studies should investigate the application of mobile data evidence during the investigative process. Thus, the research aims to answer critical investigative questions that will guide the investigator such as who, what, where, when, how, and why certain criminal activities occurred.

- The study aims to identify other persons of interest for the investigator to determine who communicated with the device.
- The research will focus on analysing the most relevant smartphone data for the investigator.
- Determining the smartphone's location at different times is challenging due to privacy concerns, therefore alternative techniques will be used to mitigate privacy concerns.

- The research aims to identify periods of activity or inactivity on the smartphone by investigating detailed application activity.
- The study will identify other devices of interest, including external connections via Wi-Fi and Bluetooth.

The model that will be developed will draw inspiration from the PADS model, introduced by Pieterse (2020), and aims to assist the investigator in quickly and more effectively constructing a timeline or rather snapshot by using both traditional and contemporary data sources to reconstruct smartphone data.

Reconstructed smartphone data can include but is not limited to:

- location data, which can assist investigators in identifying relevant evidence sources, such as surveillance footage, eyewitness accounts, and other devices in proximity at the time of the incident.
- digital footprints, such as online search history and social media activity. This can guide investigators in identifying relevant evidence sources, such as websites visited, or social media accounts used to communicate with individuals involved in the incident.

The results of this study will contribute to the growing literature and research in this field. Additionally, it will enhance the efficacy of mobile forensics in assisting investigators and facilitating the use of Android-operated smartphone data as supporting evidence in criminal investigations.

References

Alatawi, H., Alenazi, K., Alshehri, S., Alshamakhi, S., Mustafa, M., & Aljaedi, A. (2020). “Mobile Forensics: A Review”, in 2020 International Conference on Computing and Information Technology, ICCIT 2020.

Al-Hadadi, M., & AlShidhani, A. (2013). “Smartphone Forensics Analysis: A Case Study”, International Journal of Computer and Electrical Engineering, pp. 576–580.

Aziz, N.A., Mokhti, F. and Nozri, M.N.M. (2016) “Mobile Device Forensics: Extracting and Analysing Data from an Android-Based Smartphone”, in Proceedings - 4th International Conference on Cyber Security, Cyber Warfare, and Digital Forensics, CyberSec 2015. Institute of Electrical and Electronics Engineers Inc., pp. 123–128.

Dogan, S., & Akbal, E. (2017). “Analysis of Mobile Phones in Digital Forensics”, in 40th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2017, pp. 1241—1244.

Fisher v S (A51/2016) (2018), [online], https://www.saflii.org/za/cases/ZAWCHC/2018/15.html

Jones, G., Winster, S. (2017). “Forensics Analysis On Smart Phones Using Mobile Forensics Tools”, International Journal of Computational Intelligence Research, Vol 13, No.8, pp 1859–1869.

McMillan, J.E.R., Glisson, W.B. and Bromby, M. (2013) “Investigating the increase in mobile phone evidence in criminal activities”, in Proceedings of the Annual Hawaii International Conference on System Sciences, pp. 4900–4909.

Pieterse, H. (2020) Mobile forensics: “Beyond traditional sources of digital evidence”, in European Conference on Information Warfare and Security, ECCWS. Curran Associates Inc., pp. 295–303.

Statista Research Department (2023) “Market share of mobile operating systems worldwide 2009-2023”, Statistica. [online], https://www.statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009/

Taylor, P. (2023) “Mobile network subscriptions worldwide 2028”, Statistica. [online], https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

Zhang, A. et al. (2022) “Investigating the uses of mobile phone evidence in China criminal proceedings”, *Science and Justice,* Vol 62, No. 3, pp. 385–398.