Mobile Forensics: Beyond Traditional Sources of Digital Evidence

Heloise Pieterse[a]
[a]Council for Scientific and Industrial Research, Pretoria, South Africa
hpieterse@csir.co.za

Abstract: Mobility is the future and people of the 21st century are continuously witnessing the fast-paced growth of mobile technology. The ever-increasing storage capacity of mobile devices allows for the capturing of the user activities in digital format. Traditionally, such digital data include contacts, text and instant messages, call history, electronic mail, web browsing history, documents and geographical data. These rich sources of digital data present on mobile devices become increasingly important when mobile devices are linked to civil or criminal digital investigations. However, these sheer quantities of traditional digital data available on mobile devices often cause other forms of noteworthy digital data to go unnoticed. This paper investigates and identifies other available sources of digital data present on mobile devices that can be of value to digital forensic investigations. The study focuses exclusively on the Android operating system and presents an extensive evaluation of Android's file system. Furthermore, the study aims to locate, extract and utilise non-traditional or contemporary sources of digital data, such as log files, usage statistics and event data, as potential digital evidence in civil or criminal digital investigations. The outcome of the study leads to the construction of the new Pre-Analysed Device Snapshot (PADS) model, which provides a summary of the current state of the mobile device at the time of acquiring the device.

Keywords: Digital Forensics, Mobile Forensics, Android, Smartphones, Digital Evidence, Data Analysis, Modelling.

1. Introduction

Mobile devices, such as smartphones and tablet computers, have become an integral part of everyday living in the 21st century. These devices are constant companions and provide various advanced capabilities to allow end-users to perform a wide range of activities. Examples of such capabilities include cost-free communication mechanisms (e.g. Wi-Fi, Bluetooth and Near Field Communication), improved multimedia features (e.g. video recording, music playback and high-quality display) and the possibility of downloading additional applications with added functionality. These capabilities are a direct result of ever-improving hardware components and the evolution of mobile operating systems.

The reliance on and ubiquitous use of mobile devices by end-users, in conjunction with their ever-increasing storage capacity, allow for large quantities of digital data to reside in internal and external storage spaces. Such digital data includes contacts, text and instant messages, call history, geographical data, electronic mail, web browsing history and multimedia activities (Ayers et al., 2013). The evidential value offered by such traditional sources of digital data becomes increasingly important when mobile devices form part of criminal or illegal activities (Barmpatsalou, 2018). The traditional sources of digital data can help digital forensic professionals, the individual responsible to acquire, collect, preserve and analyse digital data retrieved from mobile devices (Hoelz & Maues, 2017), to form hypotheses and answer crucial questions during an investigation (Casey, 2011).

Although of great value, the sheer volume of the traditional sources of digital data often causes other contemporary forms of digital data to go unnoticed. Therefore, the purpose of this paper is to identify and discuss contemporary forms of digital data that can be potentially used as digital evidence during investigations. In order to simplify the use of contemporary digital data sources by digital forensic professionals, the paper also introduces the new Pre-Analysed Device Snapshot (PADS) model. The PADS model attempts to complement existing mobile forensic investigations by offering digital forensic professionals with a snapshot of the current state of the mobile device at the time of acquiring the device. The information produced by the PADS model will then offer guidance and direction to the digital forensic professionals during the investigation.

The efficiency of the PADS model is established by evaluating a collection of existing contemporary data present on a mobile device. The focus will be exclusively on the Android operating system since Google Android holds 74.17% of the mobile operating system market share as of December 2019 (StatsCounter,

2019). While the possibility exists to include other mobile operating systems such as iOS, the current dominance of Google Android justify the emphasis on this particular operating system. The focus of the study will be to locate, extract and utilise non-traditional or contemporary sources of digital data, such as log files, usage statistics and event data, present on Android smartphones. Such data will be provided as input to the PADS model, which in return will produce output that can be of use to an investigation as potential digital evidence.

The remainder of this paper is structured as follows. Section 2 briefly presents the forensic investigation of mobile devices and discusses the Android operating system, focussing on the current file system used by Android, as well as the most common partitions presents on Android smartphones. In Section 3, both traditional and contemporary sources of digital data are introduced and considered as potential digital evidence. Section 4 introduces the PADS model and illustrates the utilisation of contemporary digital data sources as forms of digital evidence. Section 5 concludes the paper.

2. Background

The expeditious development and growth of mobile technology continue to drive the evolution of mobile technology. These improvements coupled with their popularity among end-users ensure these devices collect and hold vast amounts of digital data. The following subsections further discuss the forensic investigation of mobile devices, with special attention given to the Android operating system as a platform often forming part of digital forensic investigations.

2.1 Mobile device forensics

Mobile devices are characterised as portable, lightweight and compact devices that provide personal computer-like functionality. Both the continuous improvements of mobile device technology coupled with the popularity of the devices among end-users ensure vast collections of digital data. Such data can become valuable sources of digital evidence, should the mobile device be linked to criminal or illegal activities. Therefore, mobile device forensic emerged to assist with the forensic investigation of mobile devices and is best described as “the science of recovering digital evidence from a mobile device under forensically sound conditions using accepted methods” (Ayers et al., 2013). The ability to capture and analyse the data present on mobile devices provides digital forensic professionals with powerful investigative capability. Attaining the available data requires of the digital forensic professional to follow the established digital forensic process, which consists of the following phases (Du, Le-Khac and Scanlon, 2017; Valjarevic & Venter, 2012):

- Planning Phase: involves the development of relevant procedures, identification of tools to be used, planning for use of appropriate human resources and the planning of all activities during other phases, which can include preparation of relevant equipment (software and hardware), infrastructure, human resources, raising awareness, training and documentation.
- Search and Seizure Phase: performed at the scene of an incident and requires the proper documentation of the entire incident scene.
- Acquisition Phase: acquiring and collecting (forensic imaging) the evidence without altering or damaging the original evidence.
- Preservation Phase: ensures the safety of collected evidence, as well as the transportation and storage of the evidence
- Analysis and Examination Phase: performs the analysis of the collected evidence and includes data filtering, validation, pattern matching and searching for particular keywords. Furthermore, this phase also conducts the identification of relationships between fragments of data, analysis of hidden data, determining the significance of the information obtained, reconstructing the event data, based on the extracted data and arriving at proper conclusions.
- Reporting Phase: involves the presentation of the results in the form of a formal report.

The presented digital forensic process provides the foundation for digital forensic professionals to investigate and obtain digital evidence from mobile devices. The Android operating system is a popular platform for mobile devices and often encountered by digital forensic professionals.

2.2 Android operating system

Operating systems form the foundation of advanced capabilities and improved functionality showcased by mobile devices today. They operate seamlessly and act as the intermediary layer between the end-user and the underlying hardware.

Google Android is an open-source mobile operating system created by the Open Handset Alliance (OHA) and officially announced in November 2007 (Lessard & Kessler, 2010). Developed for platforms such as mobile devices, the popularity of the operating system continued to grow steadily over the past decade. Part of the success of the Android operating system is the use and deployment of an appropriate file system.

YAFFS2, first released in 2004, was the primary file system for Android devices until Android version 2.2 (Froyo) (Barmpatsalou et al. 2013; Vidas et al. 2011; Zimmermann et al. 2012). However, the single-threaded design of YAFFS2 caused bottlenecks in devices released with dual-core or multi-core chipset systems (Tamma & Tindall 2015; Kim & Kim 2012). Therefore, with the release of Android version 2.3 (Gingerbread), Android switched from YAFFS2 to the extended file system (EXT) version 4 (Vidas et al. 2011; Zimmermann et al. 2012). The EXT4 file system runs smoothly on dual-core or multi-core mobile devices while providing stable performance (Kim & Kim 2012). Furthermore, the EXT4 file system also divides the disk space into logical blocks or partitions, which reduces overhead and improves throughput (Kim & Kim 2012). These key features of EXT4 make the file system ideal for newly released Android devices.

Partitioning of the file system allows the logical storage blocks, or partitions, to be accessed independently of each other and organises the stored data in a structured manner. Due to the various manufacturers of Android devices, partitioning can differ across different device models. The most common partitions of Android devices are the following (Tamma & Tindall 2015, Vidas et al. 2011):

- */boot*: holds all the information and files required by the boot process of the Android device.
- */recovery*: allows the Android device to boot into the recovery console and perform updates or maintenance operations.
- */data*: contains the bulk of user data (settings and customisations), as well as installed applications and their related data.
- */system*: holds the Android operating system, which includes libraries, system binaries and pre-installed system applications.
- */cache*: stores recovery logs, downloaded update packages and frequently accessed application data.
- */sdcard*: is found across all Android devices regardless of make or model and allows end-users to store additional files and data.

Although all partitions can hold digital data that may be of value during digital forensic investigations, digital forensic professionals usually focus on the */data*, */system* and */sdcard* partitions to obtain digital evidence.

3. Sources of digital data

The operation of mobile devices by end-users and the execution of installed applications ensure digital data is generated continuously in a deterministic and undisturbed manner (Mylonas et al, 2012). The digital data generally includes pre-generated data, data created due to the usage of the smartphone and data transferred to the device by the end-user. These various sources of digital data reside in different partitions and include both static and dynamic forms of data. Regardless of the location or nature of the digital data, the data can become valuable digital evidence should the smartphone be linked to civil or criminal investigations.

The available sources of digital data can be categorised as traditional or contemporary sources and each category is further discussed in the following subsections.

3.1 Traditional sources

Traditional sources of digital data refer to data that often form part of digital forensic investigations as digital evidence. These sources usually involve data residing on the Subscriber Identity Module (SIM) card, data created and transferred to the smartphone by the end-user and data generated by the installed applications.

Information collected on SIM cards include unique identifies (integrated circuit card identifier (ICCID) and the international mobile subscriber identity (IMSI) number), subscriber-related information and authentication keys (personal identification number (PIN) and personal unblocking key (PUK)) (Ayers et al., 2013; Curran et al.

2010; Ibrahim et al., 2016). Although all information present on SIM cards can be of value during a digital forensic investigation, the repository of subscriber information available on the SIM cards is of greater importance during the analysis and examination phases of an investigation. The available subscriber information commonly found on SIM cards include phonebook entries or contacts, text messages, call information (last numbers dialled), location area identity and service-related information (Ayers et al. 2013). However, the diminished storage capacity of SIM cards limits the amount of data that resides on the cards. Current improvements of smartphone technology allow the devices to hold larger volumes of data in internal or external storage locations.

Digital data found residing in internal or external storage locations are created as a direct result of the user's interaction with the smartphone. A small collection of the digital data present on a smartphone is user-created data, best described as data created externally to the smartphone that the end-user transfer to the device using either a wired (USB) or wireless (Bluetooth) connection. User-created data will most likely comprise of pictures, photographs, videos, audio clips and document files (i.e. presentations or spreadsheets) (Dlamini et al. 2016, Quick & Choo 2016). Other forms of user-created data also include personally identifiable information (phone number and e-mail address), accounts (Google or Apple, social media and bank) and personalised configurations (smartphone settings and themes). Although small in quantity, user-created digital data remains essential digital evidence since the data offers valuable information about the end-user.

Application-related data forms the most extensive collection of digital data present on smartphones and includes any data created or generated by smartphone applications. Smartphone applications, which consist of the user (third party) and system (pre-installed) applications, create both permanent and temporal data as the application executes (Pieterse 2019). The data is collected and stored in flat files or databases and only includes data specific to the application. These applications can act as witnesses (Pieterse & Olivier, 2014) and by analysing the collected data will provide digital forensic professionals with better context regarding the use of smartphones by end-users. Both the value and volume of application-related data emphasise the importance of such data to form part of criminal or civil investigations.

These traditional sources of digital data discussed above become valuable forms of digital evidence when the smartphones form part of criminal or civil investigations. Therefore, during analysis and examination, digital forensic professionals will pay special attention to these traditional sources of digital. However, the improvement of mobile technology and the current storage capacity of smartphones ensure various other sources of digital data is also present on smartphones.

3.2 Contemporary sources

Generally, digital forensic investigations rely on and make use of the traditional sources of digital found on mobile devices. However, various other sources of digital data exist on mobile devices that can be of value during digital forensic investigations. The purpose of this section is to explore other contemporary sources of digital data that can be found on smartphones.

3.2.1 Device logs and statistics

The first contemporary source of digital data involves collections of data relating to logging and capturing of device-specific activities and statistics. These sources of data give an overview of the activities that occurred on the smartphone and usually includes the following logged activities:

- Connections made to Wi-Fi access points or hotspots by the smartphone.
- Rebooting of the smartphone.
- Captured information regarding devices errors, irregular rebooting of the smartphone and crash logs.
- Event data such as system reboots and USB connections.

Furthermore, various statistics regarding network activities (mobile network connection, data usage per application and total data transferred) and battery usage (per application) are captured at regular intervals.

Digital forensic professionals cannot overlook the potential value of available device logs and statistics found on mobile devices. Digital forensic professionals can use such data to formulate a snapshot of the state of the smartphone, determine the location of the smartphone at the time of the acquisition, or combined the accompanying timestamps to construct a timeline, which a chronological ordering of captured events and activities. For example, digital forensic professionals can use the collected logs that captured information relating to connections made to Wi-Fi access points and hotspots to determine and pinpoint the location of

the smartphone at the time an incident occurred. Additionally, the available event data, such as USB connections made by the smartphone, can direct the digital forensic professional to other devices such as a desktop computer or laptop that may also contain important digital evidence. Therefore, digital forensic professionals must review digital data, such as the available device logs and statistics, to avoid the potential loss of valuable digital evidence.

3.2.2 User information and usage statistics

The second contemporary source of digital data focus exclusively on the end-user and captures information pertaining to usage of the smartphone and activities performed by the end-user. The data captured relating to the end-user usually includes the following:

- Profile information of the smartphone end-user (name and photograph).
- User accounts such as "Admin" and "Guest" and restrictions on the accounts.
- The most recent tasks or activities performed by the end-user.
- The most recent applications used by the end-user.
- User login details and timestamp.

The obtainable user information and usage statistics as listed above offer a detailed overview of the end-user, as well as the end-user's interaction with the smartphone. Digital forensic professionals can make use of the available user information to determine which user account was active at the time of the acquisition, as well as when the end-user logged into the account. Furthermore, chronological ordering of the recent tasks, activities and applications used by the end-user outlines to the digital forensic professional the final events that occurred before the acquisition of the smartphone. As a result, the digital forensic professional can conclude which applications were used by the end-user at the time an incident occurred. Therefore, the evaluation of the acquired digital data during the analysis and examination phases of the digital forensic investigation can be directed and prioritised based on the identified applications. Such guidance and direction during the investigation can significantly decrease the time required to conclude the analysis and the extraction of digital evidence.

3.2.3 Application information and usage

The third and final source of contemporary digital data relates specifically to additional application information such as metadata and the usage of the applications. Captured data relating to application information and usage can include the following:

- Metadata pertaining to each of the installed applications.
- Permissions and settings relating to each of the installed applications.
- Log files indicating when last the installed applications were used.
- Log files capturing the usage of the applications by the end-user.

As mentioned in Section 3.1, application-related data traditionally forms a substantial part of the digital evidence obtained from smartphones. However, additional data relating to the installed applications, as well as the usage of these applications, can offer digital forensic professionals with additional insights during a digital forensic investigation. For example, the available data showcasing the application usage can indicate to digital forensic professionals which were the most used applications used by the end-user. Such information offers guidance to the digital forensic professionals and provides direction to the digital forensic investigation during the analysis and examination phases.

4. The utilisation of contemporary digital data sources as digital evidence

Section 3 introduced and discussed both traditional and contemporary sources of digital data, highlighting the value of such data to digital forensic investigations. Currently, the utilisation of traditional digital data sources as forms of digital evidence is well understood and established. Various mobile forensic toolkits (e.g. Cellebrite and Mobile Phone Examiner Plus) exist to assist digital forensic professionals with the acquisition, preservation and analysis of digital data. Even though such mobile forensic toolkits support the acquisition of both traditional and contemporary sources of digital data from mobile devices, the analysis of the digital data is more focused on traditional sources. Overlooking the contemporary sources of digital data can cause digital forensic professionals to disregard valuable digital evidence. It becomes even more important for digital forensic professionals to consider and review other contemporary sources of digital data found on mobile

devices. Therefore, the opportunity exists for the creation of a new model that focuses specifically on the processing of contemporary digital data sources with the aim of obtaining digital evidence.

The aim of this section is to introduce a new model, called Pre-Analysed Device Snapshot (PADS) that can evaluate and utilise contemporary digital data sources. The purpose of the PADS model is to provide an overview of the mobile device at the time acquisition is performed, allowing the digital forensic professional to attain a snapshot of the current state of the mobile device. The remainder of this section discusses the inner functionality of the PADS model, as well as the practical evaluation of the PADS model using contemporary digital data collected from an Android mobile device.

4.1 Pre-Analysed Device Snapshot (PADS) model

The high-level design of the PADS model follows the input-process-output (IPO) design pattern. As input, the PADS model can receive either structured (e.g. Extensible Markup Language (XML) or log files) or unstructured (e.g. plain text files) forms of digital data. Processing of the digital data accepted as input follows four distinct steps: (1) parsing of the input into logical components, (2) extraction of the relevant logical components, (3) formulation of the extracted logical components in collections of applicable information and (4) construction of purposeful output using the obtained information with the intent to be used as potential digital evidence. The provided output group the information according to three distinct categories: (1) User, (2) Device and (3) Apps. Figure 1 illustrates the process flow of the PADS model.

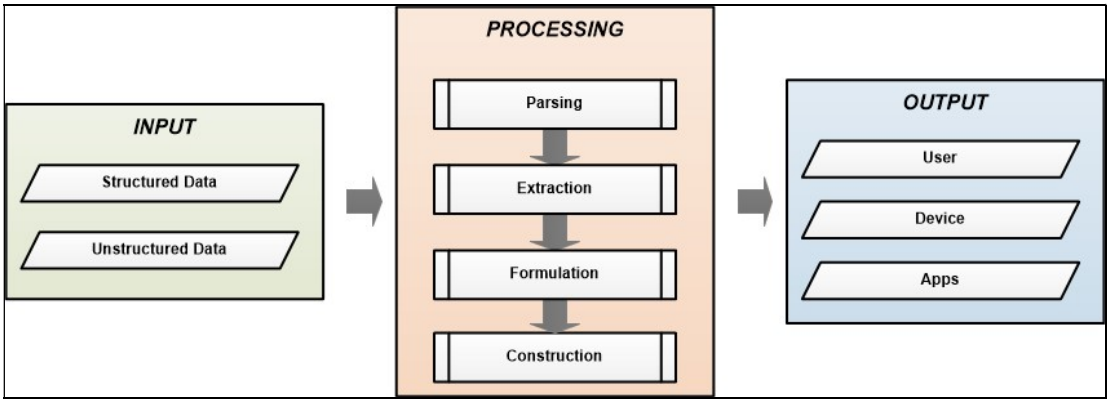

Figure 1: Illustration of the PADS Model

The PADS model expects to receive as input either structured or unstructured data sources. These data sources are contemporary digital data found on mobile devices and will include, for example, device log files and usage statistics. Once received, the PADS model proceeds to the processing phase. The parsing step is responsible to divide the received input into logical syntactic components that can easily be analysed. The extraction step will review all parsed components and extract the relevant components per pre-defined rules. These rules guide the processing of the PADS model to extract only information, such as timestamps of logged events, logged on user and last used applications, which can be of value as digital evidence. The formulation step is responsible to group the collected information into appropriate categories that best describe the state of the mobile device at the time acquisition is performed. Finally, the construction step utilises visual structures, such as timelines and graphs, to communicate the obtained information in an expressive manner. The categories forming the final output of the PADS model are the following:

- **User**: captures user-related information, such as the logged-on user and last activities conducted by the end-user. Results are illustrated using textual and visual (timeline) formats.
- **Device**: captures all events logged by the mobile device. Results are illustrated using a visual (timeline) format.
- **Apps**: captures and presents the usage of the applications by the end-user. Results are illustrated using a visual (graph) format.

The following section demonstrates the practical evaluation of the PADS model using inputs obtained from an Android mobile device.

4.2 Practical evaluation of the PADS model

The newly introduced PADS model offers needed assistance to digital forensic professionals by capturing the current state of the mobile device at the time acquisition is to be performed. However, confirming the effective use of the PADS model requires the practical evaluation of a mobile device. The test mobile device is a Samsung Galaxy S5 Mini running Android version 6.0.1 (Marshmallow). The practical evaluation involves the acquisition of the contemporary digital data sources from the test mobile device and the manual processing of the acquired data sources.

Using the test mobile device, contemporary digital data sources are acquired using traditional mobile forensic acquisition techniques. The acquired contemporary digital data sources are listed and described in Table 1.

Table 1: Collected contemporary digital data sources

Filename	Location	Description
1576540800000	/data/system/usagestats/0/daily	Plain text file capturing the usage statistics of the system applications for the past 24 hours. The file name is a timestamp that
1576108800000	/data/system/usagestats/0/weekly	Plain text file capturing the usage statistics of the system applications for the past week.
0.xml	/data/system/users	XML file capturing the user profile of the logged in user.
927_task.xml	/data/system/recent_tasks	XML file capturing information relating to the last activity performed by the logged in user.
926_task.xml	/data/system/recent_tasks	XML file capturing information relating to the second last activity performed by the logged in user.
925_task.xml	/data/system/recent_tasks	XML file capturing information relating to the third last activity performed by the logged in user.
SYSTEM_BOOT@1576575153041	/data/system/dropbox	Plain text file generated consistently at boot time, with the timestamp forming part of the file name and showing the mobile device was booted.

The collected data sources contain a combination of plain text and XML files, which will be used as input for the PADS model. Processing of the received input to attain the desired output categories is illustrated in Figure 2.

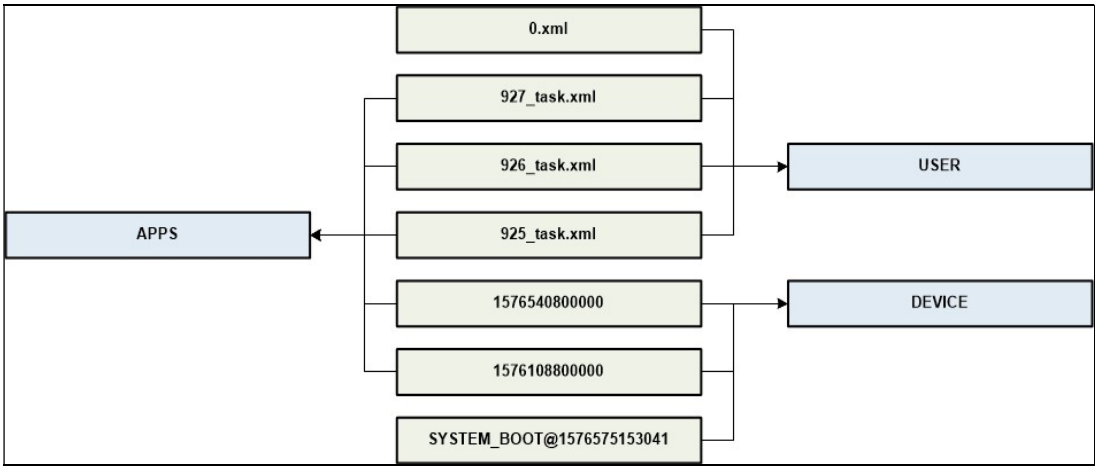

Figure 2: Selection of input to obtain the desired output

The final output produced by the PADS model is revealed in Figure 3 and presents the findings according to the categories defined in Section 4.1. All of the presented timestamps were captured in the Greenwich Mean Time (GMT) zone.

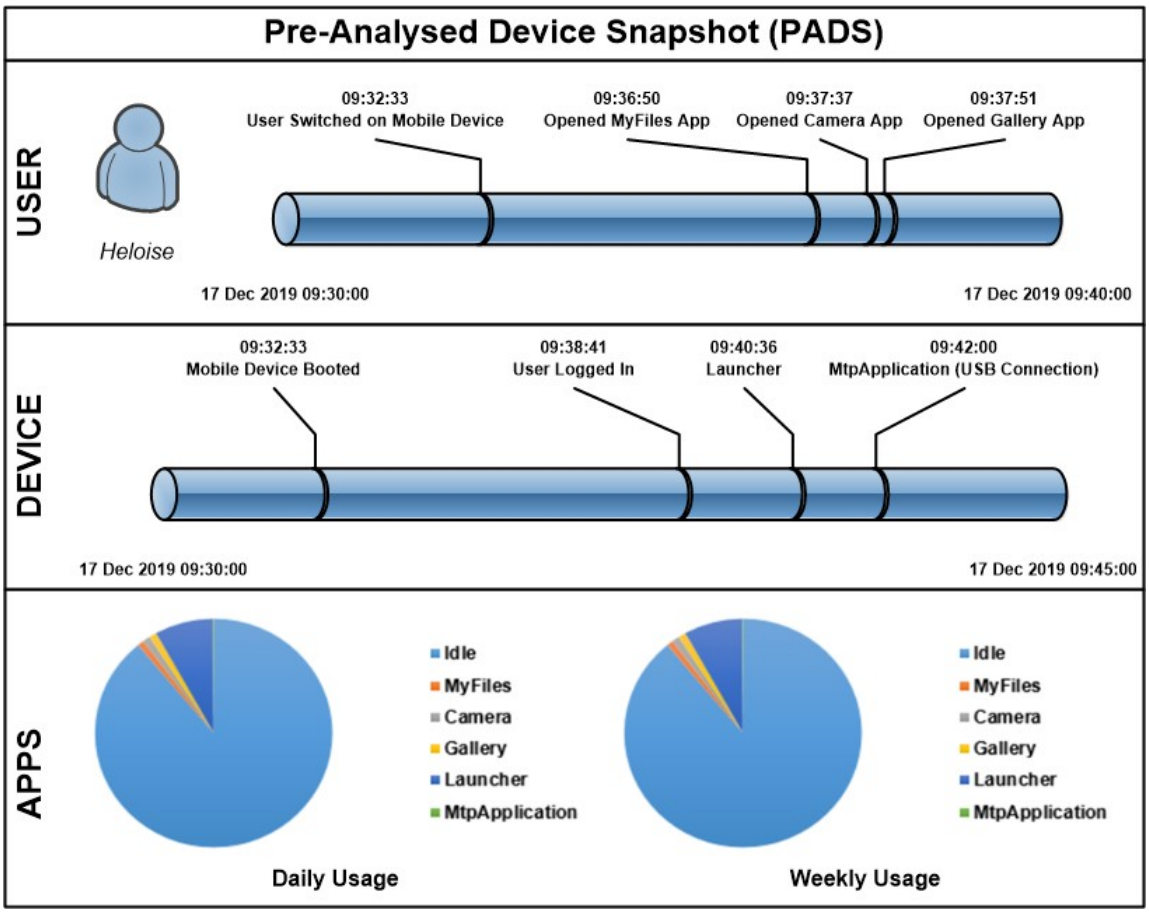

Figure 3: Visualisation of the produced output of the PADS model

The information provided as output by the PADS model showcase the state of the test mobile device at the time the practical evaluation was performed. The following information can be deduced from the received output:

- The name of the user profile logged in during the evaluation is *Heloise*.
- The end-user only used the following three applications since booting the mobile device: *MyFiles*, *Camera* and *Gallery*.
- The end-user connected the mobile device to a computer during 9:40 and 9:42 and selected the Media Transfer Protocol (MTP) option.
- Application usage for the past 24 hours is the same as the past week, signifying the mobile device was not used prior to being switched on at 9:32:33.

Digital forensic professionals can now use the findings above to guide and direct the further analysis and examination of the digital data present on the mobile device.

5. Conclusion

As a discipline, mobile device forensics provides digital forensic professionals with the necessary concepts, processes and techniques to acquire and examine digital data obtained from devices. However, the current focus of mobile device forensics concentrates on traditional sources of digital data found on mobile devices. Although the utilisation of traditional digital data sources offers digital forensic professionals adequate results, an opportunity exists to enhance the obtained digital evidence by examining contemporary digital data sources also present on mobile devices. Therefore, this paper introduced the Pre-Analysed Device Snapshot or PADS model as a method to utilise contemporary digital data sources. The PADS model provide digital forensic professionals with an overview of the state of a mobile device at the time acquisition is performed. The output

produced by the PADS model can either guide the digital forensic professional during the examination and analysis phase or be of value as digital evidence. The practical evaluation confirmed the worth of the PADS model as a method to extract additional digital evidence from mobile devices. Future work will focus on expanding the PADS model to evaluate contemporary digital data obtained from other mobile device operating systems such as iOS. Furthermore, the automation of the PADS model will also be explored to simplify the processing phase of the model.

References

Ayers, R., Brothers, S. and Jansen, W. (2013) "Guidelines on mobile device forensics (Draft)", NIST Special Publication 800-101, Technical report, National Institute of Standards and Technology.

Barmpatsalou, K., Cruz, T., Monteiro, E. and Simoes, P. (2018) "Current and future trends in mobile device forensics: A survey", *ACM Computing Surveys*, Vol. 51, No. 3, pp 1-31.

Barmpatsalou, K., Damopoulos, D., Kambourakis, G. and Katos, V. (2013) "A critical review of 7 years of mobile device forensics", *Digital Investigation*, Vol. 10, No. 4, pp 323-349.

Casey, E. (2011) *Digital evidence and computer crime: Forensic science, computers, and the Internet*, 3rd ed, Academic Press, Cambridge, Massachusetts, USA.

Curran, K., Robinson, A., Peacocke, S. and Cassidy, S. (2010) "Mobile phone forensic analysis", *International Journal of Digital Crime and Forensics*, Vol. 2, No. 2, pp 15-27.

Dlamini, Z.I., Olivier, M.S. and Grobler, M.M. (2016) The smartphone evidence awareness framework for the users, in *Proceedings of the 11th International Conference on Cyber Warfare and Security, Boston, USA, 17-18 March*, pp 439-449.

Du, X., Le-Khac, N.-A. and Scanlon, M (2017) Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service, in *Proceedings of the 16th European Conference on Cyber Warfare and Security (ECCWS 2017)*, ACPI, pp 2876-2885.

Hoelz, B. and Maues, M. (2017) Anti-forensics threat modeling, in *Peterson G., Shenoi S. (eds) Advances in Digital Forensics XIII*, Vol. 511, Springer, Berlin, Heidelberg, pp 169–183.

Ibrahim, N., Al Naqbi, N., Iqbal, F. and AlFandi, O. (2016) SIM Card Forensics: Digital Evidence, in *Annual ADFSL Conference on Digital Forensics, Security and Law*, pp 219-234.

Kim, H.-J. and Kim, J.-S. (2012) Tuning the EXT4 file system performance for Android-based smartphones, in *Sambath S., Zhu E. (eds.) Frontiers in Computer Education*, Vol. 133, Springer, Berlin, Heidelberg, pp 745-752.

Lessard, J. and Kessler, G.C. (2010) "Android forensics: Simplifying cell phone examinations", *Small Scale Digital Device Forensics Journal*, Vol. 4, No. 1, pp 1-12.

Mylonas, A., Meletiadis, V., Tsoumas, B., Mitrou, L. and Gritzalis, D. (2012) Smartphone forensics: A proactive investigation scheme for evidence acquisition, in *Gritzalis D., Furnell S., Theoharidou M. (eds.) Information Security and Privacy Research, SEC 2012*, Vol. 376, Springer, Berlin, Heidelberg, pp. 249-260.

Pieterse, H. and Olivier M. (2014) Smartphones as Distributed Witnesses for Digital Forensics, in *Peterson G., Shenoi S. (eds.) Advances in Digital Forensics X*, Vol. 433, pp 237 - 251.

Pieterse, H. (2019) *Evaluation and Identification of Authentic Smartphone Data*. PhD Thesis. University of Pretoria.

Quick, D. and Choo, K.K.R. (2016) "Big forensics data reduction: Digital forensic images and electronic evidence", *Cluster Computing*, Vol. 19, No. 2, pp 723-740.

StatsCounter (2019) "Mobile Operating Market Share Worldwide", [online], https://gs.statcounter.com/os-market-share/mobile/worldwide/2019

Tamma, R. and Tindall, D. (2015) *Learning Android Forensics*, Packt Publishing Ltd, Birmingham, UK.

Valjarevic, A. and Venter, H.S. (2012) Harmonised digital forensic investigation process model, in *Information Security for South Africa (ISSA) Johannesburg, South Africa, 15-17 August*, IEEE, pp. 1-10.

Vidas, T., Zhang, C. and Christin, N. (2011) "Toward a general collection methodology for Android devices", *Digital Investigation*, Vol. 8, pp 14-24.