Smartphone Data Evaluation Model: Identifying Authentic Smartphone Data

Abstract

Ever improving smartphone technology, along with the widespread use of the devices to accomplish daily tasks, leads to the collection of rich sources of smartphone data. Smartphone data are, however, susceptible to change and can be altered intentionally or accidentally by end-users or installed applications. It becomes, therefore, important to establish the authenticity of smartphone data, confirming the data refer to actual events, before submitting the data as potential evidence. This paper focuses on data created by smartphone applications and the techniques that can be used to establish the authenticity of the data. To identify authentic smartphone data, a better understanding of the smartphone, related smartphone applications and the environment in which the smartphone operates are required. From the gathered knowledge and insight, requirements are identified that authentic smartphone data must adhere to. These requirements are captured in a new model to assist digital forensic professionals with the evaluation of smartphone data. Experiments, involving different smartphones, are conducted to determine the practicality of the new evaluation model with the identification of authentic smartphone data. The presented results provide preliminary evidence that the suggested model offers the necessary guidance to identify authentic smartphone data.

Keywords: Smartphones, Smartphone Data, Smartphone Applications, Authenticity, Evidence, Digital Forensics, Android, iOS.

1. Introduction

Smartphones are compact devices that combine traditional mobile phone features with personal computer functionality (Kubi et al., 2011). The rapid development of smartphone technology is allowing these devices to become increasingly powerful and popular among end-users. The popularity of smartphone is the result of ever improving hardware functionality, operating systems such as Google Android and Apple iOS (Goasduff and Forni, 2017), and their associated applications. The reliance on and ubiquitous use of smartphones in daily activities of end-users have rendered these devices rich sources of data.

Data stored on smartphones, referred to as smartphone data, includes pre-generated data, data generated due to the operation of the smartphone or data transferred to the smartphone by the end-user. Smartphone data primarily resides in three locations: (i) subscriber identity module (SIM) card, (ii) internal storage, and (iii) external or portable storage such as a micro SD card (Curran et al., 2010; Al-Hadadi and AlShidhani, 2013). While all these locations contain valuable data, this research focuses on application-related smartphone data that is stored directly on smartphones. This data become important when smartphones are linked to criminal, civil, accident or corporate investigations. Smartphone data are, however, susceptible to change and can be manipulated, fabricated or altered intentionally or unintentionally by smartphone users or installed applications. The techniques, tools and processes used to intentionally compromise data are called anti-forensics (Garfinkel, 2007). Anti-forensics is best described as "any attempts to compromise the availability or usefulness of evidence to the forensic process" (Harris, 2006). It is, therefore, important for digital forensic professionals to mitigate anti-forensic actions and establish the authenticity of the smartphone data before formulating any conclusions.

Establishing the authenticity of smartphone data requires digital forensic professionals a have a better understanding of the applications responsible for creating the data. Developing a better understanding of smartphone applications can be achieved by modelling applications using recognised a reference

architecture (Pieterse et al., 2017). The reference architecture enables digital forensic professionals to easily comprehend applications and understand how the associated data originated. From the modelled smartphone applications, digital forensic professionals can also infer inconsistencies with regards to the behaviour of the applications, which impact the authenticity of the related data. Developing such an understanding of smartphone applications is only the first step to identify authentic smartphone data.

This paper, therefore, presents further requirements for smartphone data to be deemed authentic. These requirements are fully described and collected in a new model to assist digital forensic professionals with the evaluation of smartphone data. Experiments, which involve data collected from different smartphone platforms (Android and iOS), are conducted to evaluate the effectiveness of both the requirements and established model with the identification of authentic smartphone data. The outcomes of the experiments show that the requirements, along with the evaluation model, can assist digital forensic professionals and help eliminate unreliable data from being submitted as evidence before arriving at final conclusions.

The remainder of the paper is structured as follows. Section 2 highlights authenticity, describes existing techniques to detect authentic data and presents a formal description of authentic smartphone data. The requirements for authentic smartphone data are described in Section 3 and Section 4 introduces the new smartphone data evaluation model. Section 5 captures the experiments and presents the important findings. The paper closes with final discussions and conclusions summarised in Sections 6 and 7 respectively.

2. Background

Current smartphone technology equips smartphones with a collection of hardware (microphone and camera) and software (pre-installed and third-party applications) sensors that collect and store data (Mylonas et al., 2012, 2013). These sensors act as witnesses and analysing the collected data provide better

context regarding the usage of smartphones by end-users (Pieterse and Olivier, 2014). Such data can become valuable evidence should the smartphone form part of criminal, civil, accident or corporate investigations. The authenticity of the data becomes of great importance since the data can influence the accuracy of drawn conclusions (Schatz, 2007). It is, therefore, necessary for digital forensic professionals to be able to evaluate and identify authentic smartphone data. Analysing and interpreting authentic data allows for correct and accurate conclusions to be drawn.

This section further explores authenticity, describes existing techniques digital forensic professionals can use to authenticate smartphone data and presents a detailed definition of authentic smartphone data.

2.1. Authenticity

Data available on a smartphone provide digital forensic professionals with valuable insights about the interactions that took place involving the smartphone. Smartphone data are, however, vulnerable to change and can be altered, manipulated or fabricated either maliciously or by accident without leaving obvious signs (Casey, 2011; Hannon, 2014). To exclude unreliable data, digital forensic professionals must be able to establish the authenticity of smartphone data before arriving at final conclusions.

Authenticity, in common law environments, means that something is what it claims to be (Losavio, 2005) and forms part of the five fundamental requirements that must be considered when assessing the admissibility of digital evidence (Duranti and Endicott-Popovsky, 2010). Proof of authenticity is required because before digital data can be admitted into evidence, it is important to show the digital data is what it claims to be (Casey, 2011; Hannon, 2014; Losavio, 2005). Authenticity describes a digital record that has not been tampered with or corrupted, either intentionally or accidentally. An authentic digital record is, therefore, a record that (1) preserves the same identity it had when first created and (2) can be presumed or proven to have maintained its integrity over time (Cohen, 2012; Duranti, 2010). Identifying and preserving the authenticity

of digital records is a responsibility that shifts from party to party managing the records. The responsibility involves the legitimate custody of the digital records, establishing the trustworthiness of the system responsible for creating the records and various preservers handling the records, who must guarantee the authenticity over the entire life cycle of the records (Cohen, 2012).

Digital data are vulnerable to change and doubts of authenticity stem from numerous concerns such as undetectable fabrication, intentional manipulation or accidental alteration (Hannon, 2014; Losavio, 2005). The vulnerable nature of digital data makes authenticity a vital issue (Losavio, 2005). Digital data found to be not authentic must be excluded. The following section, therefore, highlights processes and techniques that can assist with the identification of authentic data, especially authentic smartphone data.

2.2. Detection of Authentic Data

Many software applications include safeguards, such as audit logs or integrity checks (Thomson, 2013), to ensure the data is valid and reliable. Such safeguards could assist digital forensic professionals to ascertain the authenticity of digital data. The focus of this paper is, however, on the processes and systems, more specifically smartphones and their related applications, responsible for creating smartphone data and determining the authenticity of that data. Smartphones and their applications generally do not have sophisticated audit logs or similar safeguards. Meanwhile, commercial mobile forensic tools, such as Cellebrite Universal Forensic Device (UFED) and FTK Mobile Phone Examiner, provide limited support in establishing authenticity (Verma et al., 2014). Therefore, new techniques and tools are required to determine the authenticity of smartphone data.

The available solutions that can assist with the identification of authentic smartphone data are few and far between. Pieterse et al. (2015) have introduced an authenticity framework for Android timestamps. The framework enables digital forensic professionals to identify authentic timestamps found on Android smartphones. The framework establishes the authenticity of timestamps found

in SQLite databases using two methods. The first method explores the Android filesystem (EXT4) for artefacts that indicate potential manipulation of the SQLite databases. The second method pinpoints inconsistencies in SQLite databases. The presence of specific file system changes and SQLite database inconsistencies are indicators that the authenticity of the stored timestamps might be compromised.

Verma et al. (2014) have proposed a technique for identifying malicious tampering of dates and timestamps in Android smartphones. The proposed technique follows a reactive approach by gathering kernel-generated timestamps of events and storing these timestamps in a secure location outside the Android smartphone. In the event of an investigation, the preserved dates and timestamps can be used to determine the authenticity of the data and timestamps extracted from the smartphone under examination.

Govindaraj et al. (2014) have designed iSecureRing, a system for securing iOS applications and preserving dates and timestamps. The system includes two modules. The first module wraps iOS applications in an additional protecting layer while the second module preserves authentic dates and timestamps of events relating to the applications.

All the solutions described above can assist digital forensic professionals with the evaluation of smartphone data, especially with regards to the authenticity of the data. However, the solutions are either platform-specific or require additional software to be installed on a smartphone prior to an investigation. Clearly, there is a need for additional solutions that can enable digital forensic professionals to determine the authenticity of smartphone data. A promising solution is to identify the requirements authentic smartphone data must adhere to. Such requirements can be derived by formally describing and defining authentic smartphone data.

2.3. Authentic Smartphone Data

The standard and intended operation of smartphones by end-users create a complex, interconnected environment that involves several components. These

components are continuously active, interacting and communicating at varying degrees. Such interaction between the components within this interconnected environment leads to the creation of digital data. Part of the digital data is persistent smartphone data, created by storage-dependent smartphone applications and stored directly on smartphones. The components operating in this environment that are directly responsible for the creation of such smartphone data are end-users' use and operation of smartphones and the installed applications, execution of those applications, and the mobile network operators.

The creation of smartphone data is best illustrated by the following two examples. The first example illustrates bidirectional communication between two smartphones. An end-user sends a text message using a messaging application installed on a smartphone. This text message is delivered to the recipient via the mobile network infrastructure, who then views the received message using a similar installed messaging application on a smartphone. The second example demonstrates unidirectional communication between an end-user and the smartphone. The end-user uses a pre-installed application to access the camera and capture a photograph that is stored on the smartphone. From the examples briefly described above, it is possible to extract the following common elements involved in the creation and management of smartphone data:

- End-user's interaction with and operation of the smartphone (open and close applications).
- End-user's usage of the installed smartphone applications to perform actions (create text messages or take photographs).
- Operation of the smartphone application to complete received actions (send text message or store photograph).
- The role of the mobile network operator as a delivery platform (deliver text message).

These common elements are collected into four core components: (i) end-user behaviour, (ii) smartphone operational state, (iii) smartphone application

behaviour and (iv) external environment. Authentic smartphone data originates as a direct result of the expected operation and normal execution of these four core components.

Authenticity, as described in Section 2.1, refers to digital data that has not been tampered with and remained unchanged over time. For smartphone data to be authentic, it is necessary that the four core components responsible for the creation and management of the data operates as expected and remain unaffected. These four components, thus, form critical pillars in maintaining the authenticity of smartphone data. Any component that is affected and operates abnormally directly impacts the authenticity of the smartphone data. It is, therefore, necessary for digital forensic professionals to be able to confirm the reliability of these components in order for the smartphone data to be deemed to be authentic.

3. Requirements for Authentic Smartphone Data

Identification of authentic smartphone data necessitates the confirmation of the standard use and operation of the core components recognised in this interconnected environment. This is possible by forming a collection of requirements that each component must adhere to. These requirements capture the expected operational behaviour of each component. Digital forensic professionals can use these requirements to assess the reliability of the components and from the established reliability, determine whether the evaluated smartphone data are indeed authentic.

3.1. End-user Behaviour

The first core component encapsulates the end-users and their use of smartphones. The focus of the requirements for this component is, therefore, aimed at the expected operation of both smartphones and the installed applications. These requirements assess the usage of the smartphone applications, the operation of the smartphone with regards to rebooting and eliminating the presence of anti-forensic applications.

3.1.1. Consistent Application Usage

The design of storage-dependent smartphone applications only permits end-users (human operator, existing smartphone application or another smartphone application) to retrieve and/or store persistent data (Pieterse et al., 2017). The end-user, using the smartphone application, must execute a collection of actions to store or retrieve the persistent data. It is, therefore, necessary to confirm the usage of the smartphone application when changes to the persistent data occurred. Intentional alterations made to the persistent data will not involve the direct usage of the smartphone application. The requirement of consistent application usage verifies the end-user used the smartphone application to access or affect changes to the persistent data. This is possible by determining an appropriate time frame that stipulates when changes to the persistent data should reflect after application usage. Such changes that falls within the pre-determined and agreed upon time frame increases the authenticity of the related smartphone data.

3.1.2. Rarely Rebooted Smartphone

The social media driven era of the 21st century requires people to always be online, connected and available (Hanna et al., 2011). Such needs cause end-users to always keep their smartphones powered and switched on. Smartphones are, therefore, not regularly turned off or rebooted. A regularly rebooted smartphone may offer an indication of potential changes made to a smartphone application's data by the end-user. A system reboot is required for intentional alterations made to smartphone data to reflect in the user interface of the smartphone application (Pieterse et al., 2016). Such a system reboot will generally occur after making the intentional changes to the persistent data. The rarely rebooted smartphone requirement evaluates timestamps associated with a system reboot. Such timestamps that follow closely after the modification of persistent data indicates the authenticity of that data may be affected.

3.1.3. Anti-forensic Applications Eliminated

Anti-forensic applications for smartphones allow end-users to destroy, hide, manipulate or prevent the creation of smartphone evidence (Sporea et al., 2012; Distefano et al., 2010). Smartphone applications, such as File Shredder (Android) or iShredder (iOS), can destroy data or data can be hidden using StegDroid or MobiStego (both Android) applications. Eliminating the presence of anti-forensic applications installed on the smartphone limits the possibility that the available smartphone data have been tampered with. It is, therefore, necessary to assess all installed applications for anti-forensic functionality, which includes the ability to hide, destroy, fabricate or manipulate smartphone data. The presence of anti-forensic applications installed on a smartphone may indicate the end-user used the applications to delete or alter smartphone data. It is, however, not a direct indication of intentional tampering of smartphone data of a specific application. Meeting the requirement of eliminating the presence of installed anti-forensic applications increases the authenticity of the related smartphone data.

3.2. Smartphone Operational State

The second core component evaluates the operational state of smartphones. The operational state of a smartphone refers to the current working state of the smartphone, which reflects how the device was used by the end-user. The focus of the requirements for this component is on the current state of the smartphone (whether the smartphone is rooted or jailbroken) and the presence of known critical files.

3.2.1. Standard Smartphone State

A standard smartphone is defined in this paper as a smartphone that is not currently and has not previously been rooted (Android) or jailbroken (iOS). Rooting an Android smartphone escalates the current rights to access the root directory (/) and allow any end-user to execute root actions (Lessard and Kessler, 2010). Jailbreaking refers to the exploitation of a flaw in the iOS operat-

ing system to remove security restrictions and obtain system-level (root) access (Egele et al., 2011). The standard smartphone state requirement evaluates the current state of the smartphone to determine if the smartphone is or has been rooted/jailbroken. Rooting/jailbreaking a smartphone provides access to smartphone partitions that are usually inaccessible to end-users, allowing access and retrieval of both smartphone applications and the corresponding data stored by the applications (Lessard and Kessler, 2010; Miller, 2011). Although not a direct indication of the intentional tampering of smartphone data, a rooted/jailbroken smartphone lacks the additional protection measures required for smartphone data to remain authentic.

3.2.2. Critical Files Present

Individuals with malicious intent that manipulate or fabricate smartphone data may attempt to impede subsequent examination of the device by removing traces created due to the intentional changes made to the data. Such traces are usually collected in user activity reports, system reboot logs, or in files associated with a specific smartphone application. The removal of these traces can potentially hide ill-intent or non-standard activities that took place on the smartphone. For this requirement, it is necessary to create a short list of critical files that must be present on a smartphone. Critical files include any file that the digital forensic professional must evaluate in order to establish the authenticity of the smartphone data. The absence of any critical file indicates that the authenticity of the smartphone data may be affected.

3.3. Smartphone Application Behaviour

The third component assesses the behaviour of installed smartphone applications. The requirements for this component are, therefore, directed at evaluating the expected behaviour of smartphones applications that operate under normal conditions. These requirements evaluate the persistent data and the storage structures responsible for storing the data of a specific smartphone application.

3.3.1. Corresponding Data (Internally)

Storage-dependent smartphone applications include actions to retrieve and/or store persistent data. Such data are made visible or accessible to the end-user by means of the user interface of the smartphone application. For smartphone data to be authentic the persistent data stored in databases or files must correspond to the data view via the user interface. This requirement confirms that the internally stored data corresponds by viewing and comparing the persistent and user interface displayed data. Evaluation of this requirement is necessary since intentional or unintentional changes made to the persistent data may not always immediately reflect in the user interface because of cached data.

3.3.2. Internal Database Consistency

Storage-dependent smartphone applications have various options to store persistent data, one of the most popular options being SQLite databases (Parihar, 2017). SQLite is an open source software library that provides a lightweight Structured Query Language (SQL) database for smartphone applications to store persistent data (Freiling et al., 2011). The main database file (.db or .db3) consists of a complete SQL structure that includes tables, indices, triggers and views (SQLite, 2017a). For the smartphone data stored in a SQLite database to be authentic, the ordering of the database records in a table must be consistent. A consistent record in a SQLite database is a record that is listed correctly when ordered according to the following fields: auto-incremented primary key and a field containing a date or timestamp. Confirming the consistency of such records is necessary since the data stored in SQLite databases can be altered or fabricated (Pieterse et al., 2015).

The requirement of internal database consistency evaluates the records of a SQLite database and identifies inconsistent records. Such inconsistent records are identifiable by executing a collection of SQL queries (Pieterse et al., 2015), which are listed in Table 1.

To preserve the integrity of the data stored in the original table, the first SQL query creates a temporary table using the CREATE TABLE statement.

Table 1: SQL queries to identify inconsistent records

Query No.	**Query**
Query 1	CREATE TABLE temp (new-id INTEGER PRIMARY KEY AUTOINCREMENT, original-id INTEGER, timestamps INTEGER);
Query 2	INSERT INTO temp (original-id, timestamp) SELECT id, date FROM table;
Query 3	SELECT T1.original-id, T1.timestamps, (T1.timestamps - T2.timestamps) AS difference FROM temp T1, temp T2 WHERE T2.new-id = T1.new-id + 1 AND difference>0;

The temporary table contains a primary key, which is an integer value that auto-increments, and all the fields that are necessary to identify the consistent SQLite database records. The second SQL query populates the temporary table with the original SQLite database records using a combination of the INSERT INTO and SELECT statements. The SELECT statement selects all the records from the table currently being evaluated while the INSERT INTO statement inserts these selected records into the temporary table. To confirm the consistency of the records collected in the temporary table, it is necessary to compare the values in the timestamp field of subsequent records. Since all the values in the timestamp field are expected to follow one another (each new record is appended at the end of the table), the difference between two subsequent values in the timestamp field must be smaller than or equal to zero. A positive difference is an indication of a timestamp that is inconsistent. The third and final SQL query performs the comparison of timestamps of subsequent records.

Applying the listed SQL queries to the SQLite database responsible for storing the persistent smartphone data allow for the identification of inconsistent records. Confirming the consistency of internal database records increases the authenticity of the related smartphone data.

3.3.3. File System Consistency

The files responsible for storing persistent data are assigned specific owners and permissions that permit modifications to occur to the data. Ownership (individual and group owners) and file permissions (read/write/execute) are assigned to the files when first created. The smartphone application responsible for creating the files is assigned ownership and is recognisable via a unique user identifier (UID). The required read/write permissions are also assigned to specifically allow the smartphone application to retrieve and/or store data. Intentional changes made to the data collected in these files will cause a change of the existing file permissions, as well as subsequent changes in the UID for the individual and/or group owners. The purpose of the file system consistency requirement is to identify changes to the ownership and file permissions of a particular smartphone application, which reflects changes made to persistent data. Identification of such changes is important since the changes impact the authenticity of the smartphone data.

3.3.4. Database File Consistency

Each SQLite database consists of the main database file and either a rollback journal or write-ahead log (WAL) file (SQLite, 2017a). The WAL approach, introduced in SQLite version 3.7.0, preserves original records in the main database file and appends changes to a separate WAL file (.db-wal), which contains a header and zero or more WAL frames (SQLite, 2017b). The file size of the main database file of a SQLite database is expected to be smaller than the size of the related WAL file. This is true for the first 1000 records accumulated since all new records are appended to the WAL file. The file size of the main database file is only expected to grow once a checkpoint occurs, causing all the records in the WAL file to be transferred to the main database file. A checkpoint, however, only occurs when the WAL file reach the limit of 1000 records (approximately 4MB in size) (SQLite, 2017b). The file size of the main database file thus remains relatively small for a time period, depending on the use of the smartphone application. An end-user with the intent to change persistent

data will cause an automatic checkpoint to occur when the main database file is opened to perform the changes. To prevent the newly made changes in the main database file from being overwritten by existing records in the WAL file, the WAL file must be deleted and the smartphone rebooted (Pieterse et al., 2015). Following a successful smartphone reboot to reflect the changes, a new WAL file is automatically generated. This new WAL file contains limited structural information and thus has a file size smaller than the file size of the main database file. The requirement of database file consistency confirms the consistent sizes of the main database file and the related WAL file, supporting the authenticity of the smartphone data.

3.4. External Environment

The final core component evaluates the environment external to the end-user and the associated smartphone. This external environment includes all other smartphones involved in bidirectional communication, as well as the mobile network operator(s). The focus of the requirements for this component is aimed at the correspondence of persistent data between different smartphones, as well as data collected by the network operator(s).

3.4.1. Corresponding Data (Externally)

Specific smartphone applications support bidirectional communication, which involves two-way communication between two smartphones such as sending text messages or making phone calls. For smartphone data to be authentic, the persistent data stored on both smartphones must correspond. This requirement confirms that the persistent data stored on two or more smartphones corresponds by viewing the stored data. Evaluation of this requirement depends on the availability of the other smartphone(s).

3.4.2. Mobile Network Operator Consistency

Mobile network operators collect detail records regrading the communication (call history/text messages) that occurred via the network. These records

prove to be valuable data to confirm bidirectional communication that transpired between two smartphones and also highlights data previously deleted from the smartphone(s). For smartphone data to be authentic, the available persistent data stored on both smartphones must correspond to the records of the mobile network operator(s). This requirement confirms that the available persistent data corresponds to the mobile network operator(s) records, should these records be available for assessment.

4. Smartphone Data Evaluation Model

The collection of requirements identified for each core component equips digital forensic professionals with the necessary instruments to evaluate the data. There is, however, no structure or order of these requirements, which can impact the effective use of the requirements during the examination of a smartphone. To assist digital forensic professionals, these requirements are captured in a smartphone data evaluation model. The smartphone data evaluation model provides a step-by-step guide to evaluate and review smartphone data. The model comprises of three phases: (i) pre-evaluation phase, (ii) smartphone evaluation phase and (iii) documentation phase. Successful completion of all three phases permits digital forensic professionals to classify the evaluated smartphone data with regards to authenticity.

4.1. Pre-evaluation Phase

The first phase of the smartphone data evaluation model requires digital forensic professionals to perform a pre-evaluation of the smartphone submitted for examination. Figure 1 presents the steps of the pre-evaluation phase. This phase first acquires and conducts an initial assessment of the smartphone to determine if the content on the smartphone is accessible and not blocked by a screen lock. A locked smartphone can impede the examination and without the required pin, password/passcode or pattern the digital forensic professional may not be able to proceed with the evaluation of the smartphone data. A

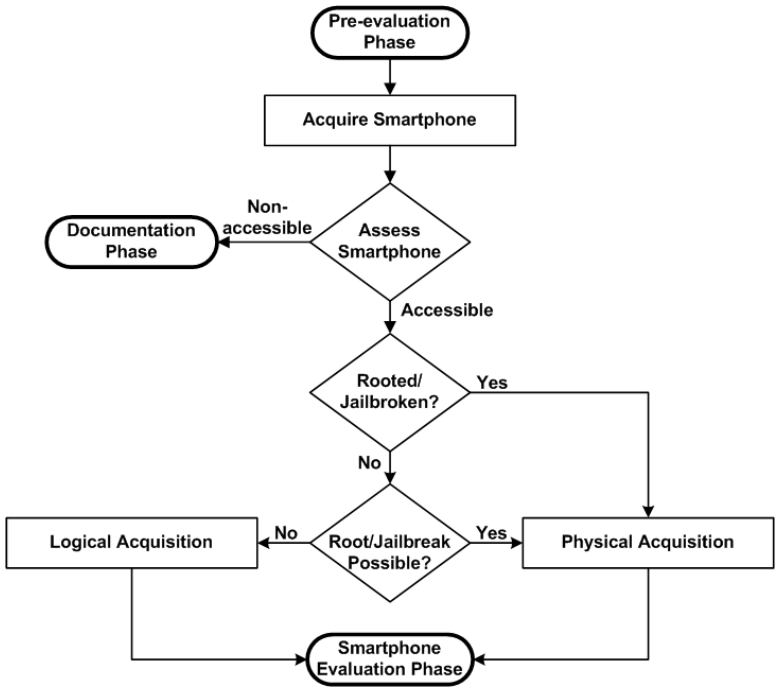


Figure 1: Pre-evaluation phase

non-accessible smartphone ultimately concludes the evaluation of the smartphone data. An accessible smartphone allows the digital forensic professional to establish the current state of the smartphone, which is necessary since the state of the smartphone will influence the course of the evaluation. The digital forensic professional can thus continue with the evaluation of the smartphone data, using either logical or physical acquisition to acquire the data.

The easiest and least intrusive manner to determine is the current state of a smartphone (rooted/jailbroken) is to view the availability of over-the-air (OTA) updates. A previously rooted/jailbroken smartphone prevents OTA updates to avoid the removal of the root/jailbreak state. Unavailable OTA updates show that a smartphone has been rooted/jailbroken but does not indicate the smartphone is currently rooted/jailbroken. A digital forensic professional can verify the current state of a smartphone via a terminal by confirming the availability of superuser/root access. Superuser/root access allows the examiner to pro-

ceed with the physical acquisition of the available smartphone data. Should a smartphone not be currently rooted/jailbroken, a digital forensic professional must investigate the feasibility of rooting/jailbreaking the smartphone using recognised and acceptable methods. Failing to root/jailbreak the smartphone will cause the examination to proceed with the logical acquisition of the smartphone data.

The outcome of the pre-evaluation phase highlights the accessibility and current state of the examined smartphone, which directs further evaluation of the smartphone data.

4.2. Smartphone Evaluation Phase

The assessment of the smartphone data continues into the smartphone evaluation phase after the pre-evaluation phase concluded and found the smartphone to be accessible for further evaluation. The evaluation of smartphone data depends, however, on the acquisition technique used to retrieve the data from the smartphone. The most popular and widely used acquisition techniques to acquire smartphone data are logical or physical acquisition techniques. Logical acquisition retrieves a bit-by-bit copy of files and directories currently stored on a smartphone (Bader and Baggili, 2010; Omeleze and Venter, 2013). Generally, this acquisition technique is unable to retrieve all of the data stored on a smartphone and is also further influenced by the underlying smartphone operating system version and current device model. Logical acquisition, therefore, limits the number of requirements that can be evaluated during this phase. Physical acquisition, however, allows for the creation of a bit-by-bit raw disk image of the entire physical store of a smartphone (Bader and Baggili, 2010; Jansen and Ayers, 2007). Selection of physical acquisition during the pre-evaluation phase will allow the digital forensic professional to obtain a copy of all the data stored on a smartphone. Thus, all of the available requirements can be evaluated.

Figure 2 illustrates the steps of the smartphone evaluation phase, which is structured according to the core components identified in Section 2.3. The first action stipulates the digital forensic professional must select a single smartphone

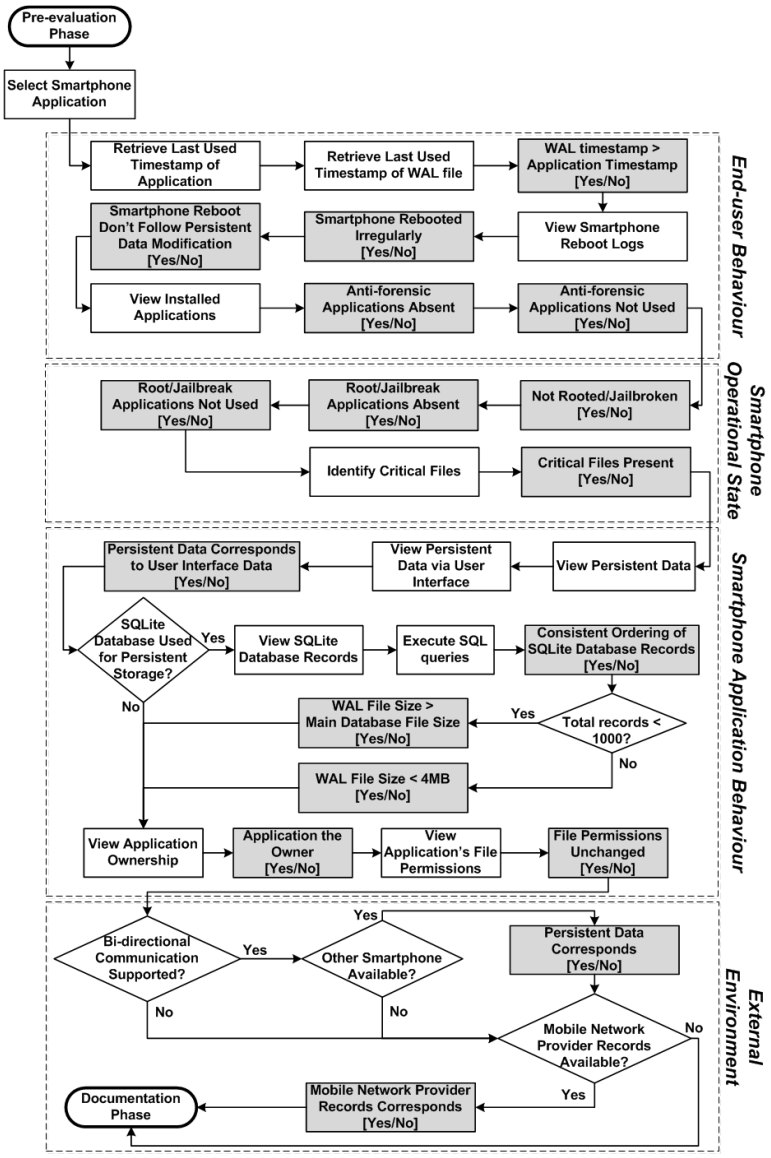


Figure 2: Smartphone evaluation phase

application to evaluate. Next, the digital forensic professional must interpret and evaluate these requirements sequentially against the collected smartphone data. Interpretation of these requirements involves three distinct actions: (i) complete a function, (ii) make an informed decision or (iii) perform a compar-

ison. The first action (white rectangular blocks) is the completion a function, which involves the viewing or retrieval of data, identification of necessary files or executing specific SQL queries. The second action (diamond-shaped blocks) requires the digital forensic professional to make an informed decision based on the evaluation of smartphone application and the related storage structure. The third action (grey rectangular blocks) involves a comparison using the collected smartphone data, which will produce a binary result [yes/no]. These comparisons are, in fact, assessment points to evaluate the established requirements and each requirement has one or more assessment points. These binary results produced by each evaluated assessment point will allow the digital forensic professional to establish the authenticity of the smartphone data.

Should the evaluation require the assessment of data from more than one smartphone application, the digital forensic professional must repeat this phase for each smartphone application. Once the digital forensic professional complete the interpretation of the requirements and collects the necessary results, the evaluation proceeds to the documentation phase to conclude the smartphone assessment.

4.3. Documentation Phase

The documentation phase captures and collects all the binary results produced by the assessment points during the smartphone evaluation phase. The produced binary result reflects either a positive [yes] or negative [no] result. A positive result confirms the specific assessment point meets the requirement while a negative result shows the assessment point contradicts the requirement. All the positive (pos_c) and negative (neg_c) results of the evaluated assessment points (n) are accumulated. Using equations (1) and (2) respectively, a score is calculated for the positive (P_s) and negative (N_s) results.

$$P_s = pos_c/n \tag{1}$$

$$N_s = neg_c/n \tag{2}$$

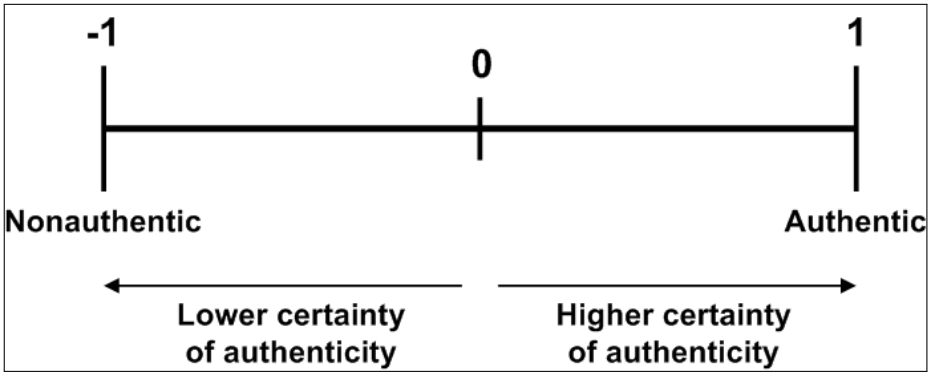


Figure 3: Probability scale to measure authenticity

$$P_s - N_s = \Delta \tag{3}$$

The calculated difference (Δ) between the two established scores, determined using equation (3), provides a probability value. Using the probability scale shown in Figure 3, the calculated probability value can be plotted to reflect whether the evaluated smartphone data are indeed authentic. In addition, the probability scale also allows the digital forensic professional to measure the certainty of the established authenticity.

This phase concludes the examination of the smartphone by collecting the established authenticity of the evaluated smartphone data, as well as key findings accumulated during the pre-evaluation and smartphone evaluation phases in a report. The digital forensic professional can use the captured results to make an informed decision regarding usage or exclusion of the data as evidence. The final decision, along with the collected results, can then be distributed to other interested parties involved in the examination of the smartphone.

5. Evaluating Smartphone Data: Conducting Experiments

The proposed smartphone data evaluation model, along with the provided requirements, allows digital forensic professionals to evaluate the authenticity of smartphone data. To ensure the effective use of the smartphone data eval-

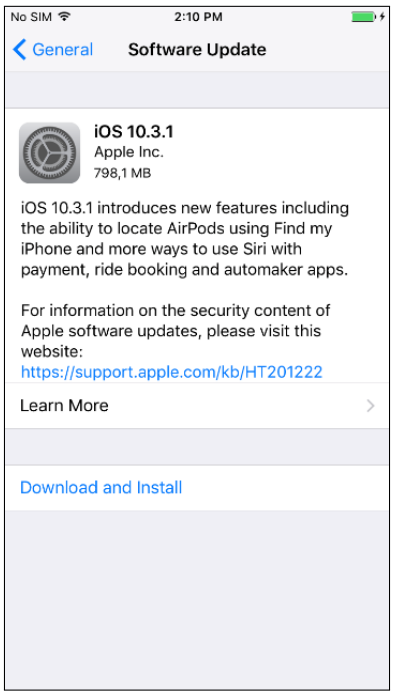


Figure 4: Availability of OTA updates on the iPhone 7

uation model and assess the model's ability to identify authentic smartphone data, additional experiments are conducted. These experiments involve smartphones running different operating systems and will evaluate both original and manipulated smartphone data.

5.1. First Experiment: Evaluate Original Smartphone Data

The objective of the first experiment is to evaluate original, non-manipulated smartphone data. The smartphone used in this experiment is an iPhone 7 running iOS version 10.0.1 and only contains data collected due to the standard or normal operation of the device. No additional or manipulated data are added to the iPhone 7. The focus of this experiment is on the default Messages application of the iOS platform that comes pre-installed on the iPhone 7.

5.1.1. Performing the Pre-evaluation Phase

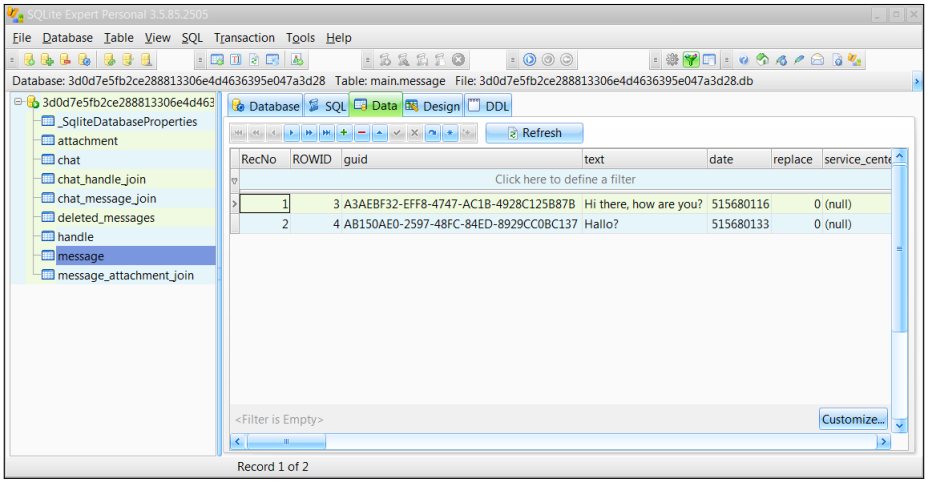
The initial steps of the pre-evaluation require the digital forensic professional to acquire and assess the iPhone 7 smartphone. On initial inspection, it is clear that the iPhone 7 is accessible and not locked by a passcode. The digital forensic professional, therefore, proceeds to verify the current state of the smartphone by viewing the availability of OTA updates. Figure 4 confirms the iPhone 7 allows OTA updates and is thus not currently jailbroken. Since the iPhone 7 has not been previously jailbroken, the digital forensic professional needs to verify whether it is possible to jailbreak the iPhone 7 and obtain superuser/root access. Reviewing the jailbreaking techniques available at the time of writing revealed no acceptable solution to jailbreak iOS version 10.0.1 running on iPhone 7. Retrieving the smartphone data from the iPhone 7 is, therefore, done using logical acquisition. The iTunes backup utility (Bader and Baggili, 2010) is used to perform the logical acquisition of the smartphone data from the iPhone 7.

5.1.2. Evaluate the Smartphone Data

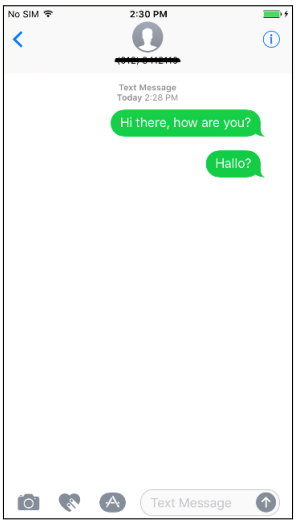
The first step of the smartphone evaluation phase requests the selection of a smartphone application. The focus of this experiment, as mentioned previously, is on the default Messages iOS application. The Messages application, as well as the applications related data, forms the focus of the smartphone evaluation phase. The logical acquisition of the iPhone 7 smartphone data limits the requirements digital forensic professionals can evaluate during the smartphone evaluation phase. The acquired smartphone data permits the assessment of the following four requirements: anti-forensic applications eliminated, standard smartphone state, internal database consistency and corresponding data (internally).

Reviewing the applications currently installed on the iPhone 7 and comparing the core functionality of these applications against known anti-forensic capabilities (hide, destroy, fabricate or manipulate) confirmed no anti-forensic applications are installed. The results produced by the pre-evaluation phase verified the availability of OTA updates and thus the iPhone 7 is not and has

not previously been jailbroken. It is, therefore, not necessary to search for and confirm the presence of jailbreak-specific applications. The iTunes backup utility supports the acquisition of the SQLite database that holds the persistent data of the Messages application. The digital forensic professional confirms the internal database consistency by viewing the SQLite database records of the



(a) UI view



(b) Database view

Figure 5: Corresponding Data of the iPhone's Messages application

Messages application (sms.db) using a SQLite manager and executing the SQL query listed in Section 3.3.2. The result of the query shows a consistent ordering of the SQLite records. Finally, the digital forensic professional confirms the data stored in the SQLite database corresponds to the data shown in the user interface (UI) of the Messages application. Figure 5 substantiate this finding by comparing the messages displayed via the user interface of Messages application to the messages stored in the database.

5.1.3. Findings

The evaluation of the acquired smartphone data from the iPhone 7 and the assessment of the available requirements corroborate the following findings. Firstly, reviewing the available smartphone applications showed that there are no anti-forensic applications installed on the iPhone 7. Secondly, the availability of OTA updates confirms that the iPhone 7 is not and has not previously been jailbroken. Thirdly, viewing the records of the SQLite database associated with the Messages application revealed a consistent ordering of these records, which also corresponds to the data when viewed via the user interface.

In total seven assessment points spread across four requirements were evaluated during this experiment, all which produced positive results. Using the equations defined in Section 4.3, the calculated probability value for the evaluated smartphone data is 1. Visualised on the probability scale shown in Figure 3, the probability value confirms the authenticity of the evaluated smartphone data. It is, however, not possible to fully confirm the authenticity of the evaluated smartphone data since only a subset of the necessary requirements were assessed.

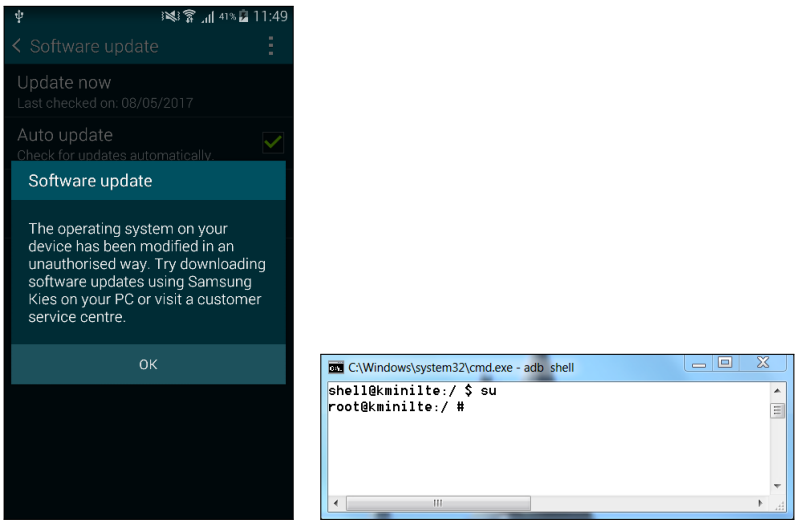
Based on this calculated probability value the digital forensic professional can conclude the smartphone data associated with the Messages application is original and authentic with a higher certainty. This established level of certainty will, therefore, guide the digital forensic professionals regarding the submission and use of the smartphone data as potential evidence to draw conclusions.

5.2. Second Experiment: Evaluate Manipulated Smartphone Data

The findings collected during the first experiment showed that the smartphone data evaluation model provides digital forensic professionals with the necessary tools to evaluate the authenticity of smartphone data. Even though only a small collection of data was retrieved from the iPhone 7 using the logical acquisition technique, the limited data acquired did not impact the effective evaluation capability of the model. Based on the findings captured using the model, digital forensic professionals could still establish the authenticity of the evaluated smartphone data. The focus of the first experiment was, however, to confirm the authenticity of original and non-manipulated smartphone data. It is also necessary to validate the effective use of the model evaluating and identifying potentially manipulated smartphone data. Pieterse et al. (2015) demonstrated the successful manipulation of data stored on Android smartphone.

The steps to manipulate Android smartphone data stored in SQLite databases are as follows:

1. Root the Android smartphone.
2. Copy the .db and .db-wal SQLite database files of the selected Android application to the /sdcard/ location on the Android smartphone.
3. Copy the .db and .db-wal SQLite database files from the /sdcard/ location to the computer.
4. Use a SQLite viewer to alter the data stored in the SQLite database.
5. Remove the .db and .db-wal SQLite database files from the Android smartphone using the rm command.
6. Copy the .db SQLite database file containing the manipulated data to the Android smartphone.
7. Move the .db SQLite database file to /database/ location of the Android application.
8. Change the permissions of the .db SQLite database file using the chmod 666 command.
9. Reboot the Android smartphone.



(a) OTA updates (b) Superuser/root access permitted

Figure 6: Pre-evaluation of the Android smartphone

The second experiment explores the evaluation of manipulated smartphone data on an Android smartphone (Samsung Galaxy S5 Mini) running Android version 6.0.1. The focus of this experiment is on the default Messaging application of the Android platform that comes pre-installed on Android devices.

5.2.1. Performing the Pre-evaluation Phase

The initial steps of the pre-evaluation require the digital forensic professional to acquire and assess the Android smartphone. On initial inspection, it is clear the Android smartphone is accessible and not locked by a pin, pattern or password. The digital forensic professional, therefore, proceeds to verify the current state of the smartphone by viewing the availability of OTA updates. Figure 6 (a) shows the Android smartphone prevents OTA updates and is either currently or has been previously rooted. Attempting to access the Android smartphone using the superuser (su) command showed that the device is indeed currently rooted, which is substantiated by Figure 6 (b). Retrieving the smartphone data from the Android smartphone is, therefore, performed using physical acquisition. The dd utility command is used to obtain a physical image of the Android

smartphone (Lessard and Kessler, 2010).

5.2.2. Evaluate the Smartphone Data

The first step of the smartphone evaluation phase once again requests the selection of a smartphone application. The focal point of this experiment, as mentioned above, is on the default Messaging application of the Android platform. The Messaging application, as well as the application's related data, forms the focus of the smartphone evaluation phase. The physical acquisition of the Android smartphone data allows the digital forensic professional to evaluate all of the requirements during the smartphone evaluation phase.

The first segment of the smartphone evaluation phase assesses the end-user's behaviour in terms of application usage, rebooting of the smartphone and presence of anti-forensic applications. The available log files in the usagestats folder (/data/system/usagestats/0) indicate when an application was last used. The timestamps are captured for daily, weekly, monthly and yearly intervals. The name of each log file in the usagestats folder is a timestamp that indicates when the collection of data began. The last time of usage for each application is then calculated using the filename and the lastTimeActiveSystem or event value. Analysis of the newest log file created in the daily/ folder, which is presented in Figure 7, shows the message composer activity of the Messaging application (com.android.mms.ui.ConversationComposer) was last accessed on August 1, 2017, at 20:50:41.774 GMT+02:00 to send a text message. Reviewing the timestamps of the .db-wal file associated with the default Messaging application, shown in Figure 8 (b), contradicts the log entry in the captured usagestats log file, since, the timestamp of the .db-wal file (August 1, 2017, at 21:01.00

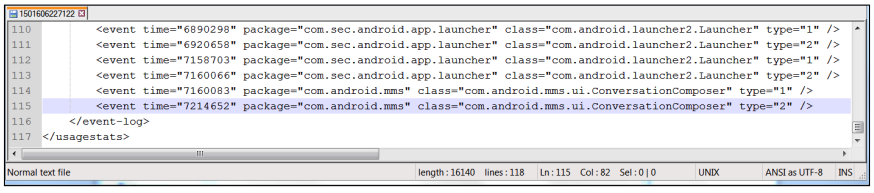
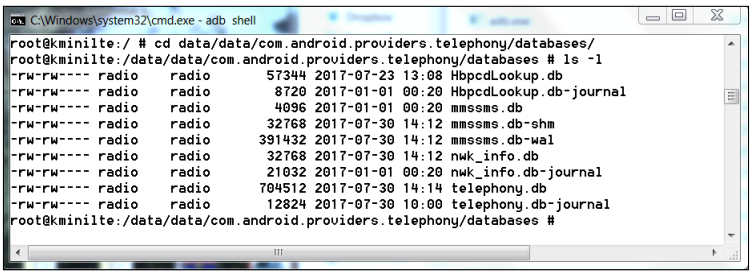
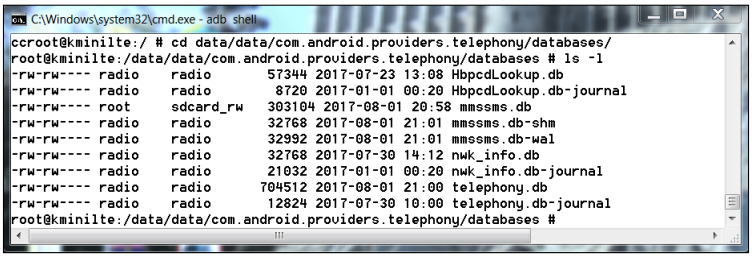


Figure 7: Snippet of the usagestats file



(a) Original



(b) Manipulated

Figure 8: Comparison of the original and manipulated mmssms.db files

GMT+02:00) does not follow in an appropriate time frame after the last usage of the Messaging application. Next, the digital forensic professional views the system reboot logs (/data/system/dropbox/) to determine if and when the Android smartphone was rebooted. Based on the large collection of available SYSTEM_BOOT@[timestamp].txt files, it is clear the Android smartphone was regularly rebooted by the end-user. On closer inspection, the digital forensic

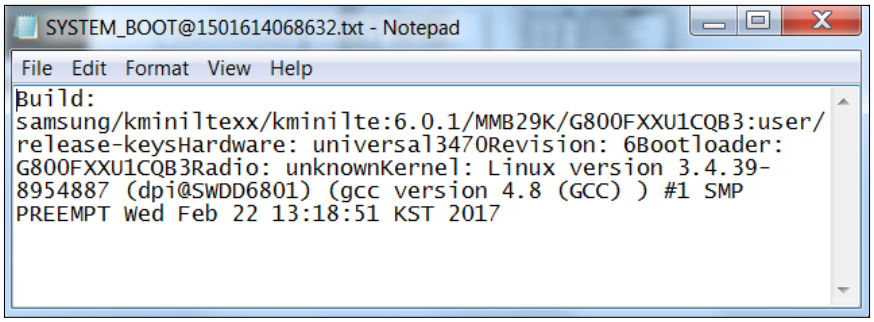


Figure 9: Snapshot of the SYSTEM_BOOT@1501614068632.txt log file

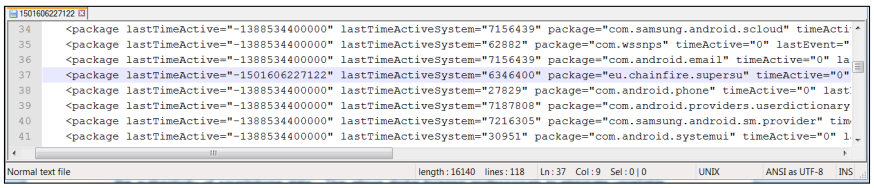


Figure 10: Snippet of the usagestats file

professional found a system reboot (see Figure 9) that occurred shortly after the modification of the Messaging SQLite database on August 1, 2017, at 21:01:08.632 GMT+02:00. Reviewing the applications currently installed on the Android smartphone and comparing the core functionality of these applications against known anti-forensic capabilities (hide, destroy, fabricate or manipulate) eliminated the presence of anti-forensic applications.

The second segment of the smartphone evaluation phase assesses the operational state of the Android smartphone and confirms the presence of known critical files. The results produced by the pre-evaluation phase verified that the Android smartphone is currently rooted. This is further confirmed by the usage of the SuperSu application, which is logged in the usagestats file. Figure 10 provides a snippet of the usagestats file, showing the SuperSu application was last used on August 1, 2017, at 20:36:13.522 GMT+02:0. During the next step, the digital forensic professional confirms the existence of the critical files on the Android smartphone, which includes the usagestats and system reboot log files.

The third segment of the smartphone evaluation phase assesses the behaviour of the Messaging application. The Messaging application uses a SQLite database for persistent storage of data. It is, therefore, possible to view the stored records and evaluate the following four requirements: corresponding data (internally), internal database consistency, file system consistency and database file consistency. Firstly, the digital forensic professional found the records stored in the mmssms.db SQLite database corresponds with the text messages shown in the user interface of the Messaging application. To confirm the consistency of the SQLite database records, the examiners view the database records and execute the query specified in Section 3.3.2. The result produced by the queries con-

RecNo	_id	thread_id	person	date	date_se...	protocol	read	status	type	reply...	su...	body
Click here to define a filter												
1	1	1	(null)	1501416757316	1501416	0	1	-1	1	0	(null	MASSIVE UNRESERVED AUCTION TODAY @ 11AM
2	12	7	(null)	1501420570123	1501420	0	1	-1	1	0	(null	1234
3	13	2	(null)	1388534494809	1501508	0	1	-1	1	0	(null	Increase your chances to WIN double 3D Movie Tic
4	14	3	(null)	1501612546881	0	(null)	1	-1	2	(null)	(null	Hallo. This is a new text message.
5	15	3	(null)	1501613414397	0	(null)	1	-1	2	(null)	(null	Another message
6	16	3	(null)	1501613414397	0	(null)	1	-1	2	(null)	(null	Another message THAT HAS BEEN MANIPULATED

Figure 11: mmssms.db SQLite database records

firmed that the records are consistent and ordered correctly. Next, the digital forensic professional is able to identify changes to the file permissions and ownership of the main SQLite database file of the Messaging application (see Figure 8). Viewing the mmssms.db SQLite database reveals a total of 6 records currently collected in the database (see Figure 11). The size of the mmssms.db-wal file is thus expected to be greater than the size of the mmssms.db file, since a checkpoint has not yet occurred. Figure 8 (b) contradicts this requirement and shows that the mmssms.db-wal file size to be greater than the mmssms.db file size.

The final segment of the smartphone evaluation phase assesses the environment external to the smartphone. Although this application does support bi-directional communication, the other smartphones involved, as well as the captured mobile network operator logs, were not available for evaluation. Therefore, the digital forensic professional concludes the evaluation of the Android smartphone.

5.2.3. Findings

The evaluation of the smartphone data acquired from the Android smartphone and the assessment of the available requirements corroborate the following findings. Firstly, the end-user rooted the Android smartphone and previously used the installed SuperSu application. Secondly, the Android smartphone was regularly rebooted, with a reboot following closely after the changes occurred to the Messaging SQLite database. Thirdly, changes to the ownership of the main SQLite database file of the Messaging application were identified. Fourthly, the usage of the Messaging application contradicts the expected behaviour. Finally,

the file size of the .db-wal file was found to be inconsistent based on the number of records currently stored in the SQLite database.

In total 13 assessment points across nine requirements were evaluated during this experiment. Of the evaluated assessment points, only 38% produced a positive result. Using the equations defined in Section 4.3, the calculated probability value for the evaluated smartphone data is -0.2. Visualised on the probability scale shown in Figure 3, the probability value reflects a lower certainty of authenticity.

Based on the assessment of the available smartphone data and the interpretation of all the evaluated requirements, the digital forensic professional can conclude that the text messages stored by the Messaging application on the Android smartphone may have been altered or tampered with. It is, therefore, not possible to classify the evaluated smartphone as authentic.

6. Discussion and Future Work

The vulnerable nature of digital data, such as smartphone data, necessitates the ability to evaluate the authenticity of smartphone data. This allows digital forensic professionals to eliminate unreliable data from being submitted as potential evidence. Authentic smartphone data requires the core components (end-user behaviour, smartphone operational state, smartphone application behaviour and external environment) responsible for the creation and management of smartphone data to operate as expected and remain unaffected. The reliability of these components can be confirmed by a unique collection of requirements. The collective validation of requirements increases the authenticity of the evaluated smartphone data.

The diverse collection of requirements must be organised into a purposeful model to provide proper assistance to digital forensic professionals evaluating smartphone data. The smartphone data evaluation model follows a simple structure that offers digital forensic professionals a step-by-step guide to evaluate the smartphone data of an application. The model equips digital forensic profession-

als with the necessary techniques and knowledge to establish the authenticity of smartphone data, which leads to correct and accurate conclusions to be drawn from the data. Digital forensic professionals can, therefore, make an informed decision regarding the inclusion or exclusion of smartphone data as potential evidence. Using this model will potentially save digital forensic professionals valuable time and quicken the assessment of the authenticity of smartphone data.

The identified requirements and formulated model are, however, not a flawless solution. The requirements cannot directly identify or pinpoint fabricated or manipulated smartphone data. Evaluating smartphone data using these requirements will only provide the digital forensic professional with the necessary guidance to establish the overall authenticity of the data. The final decision regarding the inclusion or exclusion of smartphone data based on the data's evaluated authenticity still remains with the digital forensic professional. It is also important for the collection of requirements to be continuously reviewed and updated as smartphone technology evolves. Such reviews can lead to the identification of additional requirements, adjustment of existing requirements or the removal of requirements that are no longer applicable.

Future work will continue to expand this research and will explore other techniques to further establish the authenticity of smartphone data. The requirements and the smartphone data evaluation model introduced in this paper will be used to create a smartphone data classification model, which will provide digital forensic professionals with a calculated outcome that can classify the authenticity of smartphone data according to various levels of certainty. The classification model will be evaluated using various experiments that include both authentic and manipulated smartphone data.

7. Conclusion

The proliferation and popularity of smartphones lead to the creation and availability of large quantities of smartphone data. Smartphone data are, how-

ever, susceptible to change, which can be caused by anti-forensic tools, malware or users with malicious intent. It is, therefore, necessary to establish the authenticity of smartphone data and ensure the data originated as a result of the expected operation of the smartphone and the normal behaviour of the related smartphone application. This paper formally defined authentic smartphone data and from the definition identified a collection of requirements that can evaluate the authenticity of smartphone data. These requirements are accumulated into a new model, called the smartphone data evaluation model, to assist digital forensic professionals with the evaluation of smartphone data. The experiments performed involved different smartphone platforms (iPhone and Android) and revealed that the model can assist digital forensic professionals with the evaluation of both original and manipulated smartphone data. Using the smartphone data evaluation model allows a digital forensic professional to ensure the smartphone data refer to actual events and permits the elimination unreliable smartphone data. Submitting authentic smartphone data as evidence will allow digital forensic professionals to formulate accurate conclusions.

References

Al-Hadadi, M., AlShidhani, A., 2013. Smartphone forensics analysis: A case study. International Journal of Computer and Electrical Engineering 5, 576–580.

Bader, M., Baggili, I., 2010. iPhone 3GS forensics: Logical analysis using Apple iTunes backup utility. Small Scale Digital Device Forensics Journal 4, 1–15.

Casey, E., 2011. Digital evidence and computer crime: Forensic science, computers, and the Internet. Academic press.

Cohen, F.B., 2012. Digital forensic evidence examination. Fred Cohen & Associates.

Curran, K., Robinson, A., Peacocke, S., Cassidy, S., 2010. Mobile phone forensic analysis. International Journal of Digital Crime and Forensics 2, 15–27.

Distefano, A., Me, G., Pace, F., 2010. Android anti-forensics through a local paradigm. Digital Investigation 7, 83–94.

Duranti, L., 2010. From digital diplomatics to digital records forensics. Archivaria, The Journal of the Association of Canadian Archivists 68, 39–66.

Duranti, L., Endicott-Popovsky, B., 2010. Digital records forensics: A new science and academic program for forensic readinees. Journal of Digital Forensics, Security and Law 5, 45–62.

Egele, M., Kruegel, C., Kirda, E., Vigna, G., 2011. PiOS: Detecting privacy leaks in iOS applications., in: NDSS, pp. 177–183.

Freiling, F., Spreitzenbarth, M., Schmitt, S., 2011. Forensic analysis of smartphones: The Android Data Extractor Lite (ADEL), in: Proceedings of the Conference on Digital Forensics, Security and Law, pp. 151–160.

Garfinkel, S., 2007. Anti-forensics: Techniques, detection and countermeasures, in: Proceedings of the 2nd International Conference on i-Warfare and Security, pp. 77–84.

Goasduff, L., Forni, A., 2017. Gartner says worldwide sales of smartphones grew 7 percent in fourth quarter of 2016. URL: `http://www.gartner.com/newsroom/id/3609817`.

Govindaraj, J., Verma, R., Mata, R., Gupta, G., 2014. Poster: iSecureRing: Forensic ready secure iOS apps for jailbroken iPhones, in: 35th IEEE Symposium on Security and Privacy.

Hanna, R., Rohm, A., Crittenden, V.L., 2011. We're all connected: The power of the social media ecosystem. Business horizons 54, 265–273.

Hannon, M., 2014. An increasingly important requirement: Authentication of digital evidence. Journal of the Missouri Bar 70, 314–323.

Harris, R., 2006. Arriving at an anti-forensics consensus: examining how to define and control the anti-forensics problem. Digital Investigation 3, 44–49.

Jansen, W., Ayers, R., 2007. Guidelines on cell phone forensics. NIST Special Publication 800.

Kubi, A., Saleem, S., Popov, O., 2011. Evaluation of some tools for extracting e-evidence from mobile devices, in: Application of Information and Communication Technologies (AICT), pp. 1–6.

Lessard, J., Kessler, G., 2010. Android forensics: Simplifying cell phone examinations. Small Scale Digital Device Forensics Journal 4, 1–12.

Losavio, M., 2005. Non-technical manipulation of digital data. Advances in Digital Forensics 194, 51–63.

Miller, C., 2011. Mobile attacks and defense. IEEE Security & Privacy 9, 68–70.

Mylonas, A., Meletiadis, V., Mitrou, L., Gritzalis, D., 2013. Smartphone sensor data as digital evidence. Computers & Security 38, 51–75.

Mylonas, A., Meletiadis, V., Tsoumas, B., Mitrou, L., Gritzalis, D., 2012. Smartphone forensics: A proactive investigation scheme for evidence acquisition, in: IFIP International Information Security Conference, Springer. pp. 249–260.

Omeleze, S., Venter, H.S., 2013. Testing the harmonised digital forensic investigation process model-using an Android mobile phone, in: Information Security for South Africa, 2013, IEEE. pp. 1–8.

Parihar, A., 2017. Five of the most popular databases for mobile apps. URL: `http://blog.trigent.com/five-of-the-most-popular-databases-for-mobile-apps/`.

Pieterse, H., Olivier, M., 2014. Smartphones as distributed witnesses for digital forensics. Advances in Digital Forensics X 433, 237–251.

Pieterse, H., Olivier, M., van Heerden, R., 2017. Evaluating the authenticity of smartphone evidence. Advances in Digital Forensics XIII 511, 41–61.

Pieterse, H., Olivier, M.S., van Heerden, R.P., 2015. Playing hide-and-seek: Detecting the manipulation of Android timestamps, in: Information Security for South Africa (ISSA), 2015, IEEE. pp. 1–8.

Pieterse, H., Olivier, M.S., van Heerden, R.P., 2016. Reference architecture for Android applications to support the detection of manipulated evidence. SAIEE Africa Research Journal 107, 92–103.

Schatz, B., 2007. Digital evidence: representation and assurance. Ph.D. thesis. Queensland University of Technology.

Sporea, I., Aziz, B., McIntyre, Z., 2012. On the availability of anti-forensic tools for smartphones. International Journal of Security (IJS) 6, 58–64.

SQLite, 2017a. Database file format. URL: `www.sqlite.org/fileformat.html`.

SQLite, 2017b. Write-ahead logging. URL: `www.sqlite.org/wal.html`.

Thomson, L.L., 2013. Mobile devices: New challenges for admissibility of electronic evidence. SciTech Lawyer 9, 32.

Verma, R., Govindaraj, J., Gupta, G., 2014. Preserving dates and timestamps for incident handling in Android smartphones. Advances in Digital Forensics X 433, 209–225.