Chapter 1

CLASSIFYING THE AUTHENTICITY OF EVALUATED SMARTPHONE DATA

Heloise Pieterse, Martin Olivier and Renier van Heerden

Abstract Advances in smartphone technology coupled with the widespread use of such devices to accomplish daily tasks create valuable sources of smartphone data. Such data becomes increasingly important when smartphones are linked to civil or criminal investigations. As with all forms of digital data, smartphone data is susceptible to change due to intentional or accidental alterations by end-users or installed applications. It is, therefore, essential to establish the authenticity of smartphone data, before submitting the data as potential evidence. Previously conducted research formulated the smartphone data evaluation model, which provides a methodological approach for evaluating the authenticity of smartphone data. However, the smartphone data evaluation model only stipulates how to evaluate smartphone data without providing a formal outcome regarding the authenticity of the data. This paper introduces a new classification model that presents the grade of authenticity of evaluated smartphone data, as well as the completeness of the evaluation. The outcome of a practical experiment confirms the effective use of the classification model to classify the authenticity of smartphone data.

Keywords: Digital forensics, smartphone forensics, smartphones, smartphone data, authenticity.

1. Introduction

The competitive nature of the global smartphone market [1] causes continuous technological advancements in smartphone technology. These advancements enable existing smartphone models to support different operating systems, as well as permit the installation of various third-party applications. The current capabilities of smartphones coupled with their widespread use to perform daily activities lead to rich collections of smartphone data. Smartphone data "includes any data of

probative value that is generated by an application or transferred to the smartphone by the end-user" [2]. Generally, smartphone data describes events that occurred on the smartphone and the associated timestamps support the chronological ordering of these events [3]. Therefore, such data becomes a valuable form of digital evidence, especially when linked to civil or criminal investigations.

Smartphone data is, however, susceptible to change [4]. Changes to smartphone data can occur due to the execution of incorrect or error-prone applications or deployed malware. Furthermore, end-users with malicious intent can alter smartphone data intentionally. Intentional changes to smartphone data are commonly referred to as anti-forensics, which is used to "compromise the availability or usefulness of evidence to the forensic process" [5] while several recent research studies [6, 7] have successfully demonstrated the manipulation, fabrication and alteration of smartphone data. Unknown or unexpected changes to existing smartphone data that remains undetected can cause misleading results when analysed. Therefore, it becomes essential for digital forensic professionals to detect such changes by establishing the authenticity of the smartphone data before formulating any conclusions [8]. Authenticity commonly refers to the preservation of data from the time it was first generated and the ability to prove that the integrity of the data has been maintained over time [9–12].

Establishing the authenticity of smartphone data necessitates a better understanding of the environment the smartphone operates in and the key components responsible for creating smartphone data. These components include the smartphone application responsible for creating the data, the operation of the smartphone by the end-user and the impact of the immediate surroundings. Previous research performed by Pieterse et al. [13] formally described authentic smartphone data and from the description deduced a collection of requirements to evaluate the authenticity of such data. These requirements were then used to construct the smartphone data evaluation model, which provides digital forensic professionals with a structured approach for evaluating the authenticity of smartphone data. However, the purpose of the smartphone data evaluation model is to offer guidance and stipulate how to evaluate smartphone data. The results produced by the smartphone data evaluation model excludes any formal classification of the authenticity of the evaluated data. Furthermore, existing classification scales for digital evidence, such as Casey's certainty scale or degrees of likelihood (almost definitely, most probably, probably, very possible or possibly) [9], focus more on the certainty of drawn conclusions. Following a more formal

and consistent methodology to classify the authenticity of smartphone data can add further support to the certainty of drawn conclusions.

This paper introduces a new classification model for smartphone data, constructed using the smartphone data evaluation model and the requirements available to evaluate the authenticity of such data. The classification model classifies evaluated smartphone data using an ordered pair of values. The first value represents the grade of authenticity while the second value describes the completeness of the evaluation. Collectively, the classification allows digital forensic professionals to present the authenticity of evaluated smartphone data with particular confidence. Conducting a practical experiment involving the manipulation of smartphone data on an iPhone 7 confirms the effective use of the classification model to classify the authenticity of the data.

The remainder of this paper is structured as follows. Section 2 discusses authentic smartphone data, the requirements to evaluate such data and the previously designed smartphone data evaluation model. The focus of Section 3 is on the newly formulated classification model while Section 4 presents the Smartphone Application Data Authenticity Classifier (SADAC), a software application designed to simplify the evaluation and classification of smartphone data. The paper closes with final discussions and conclusions summarised in Section 5.

2. Background

Detailed analysis of smartphone data offers contextual information about the end-user, as well as the activities performed using the smartphone. Therefore, such data can be valuable digital evidence should the smartphone form part of civil or criminal investigations. The authenticity of smartphone data becomes of great importance to ensure digital forensic professionals draw correct and accurate conclusions from the data. Formulating correct conclusions requires digital forensic professionals to be able to review smartphone data and evaluate the authenticity of such data. The smartphone data evaluation model introduced by Pieterse et al. [13] offers a methodological approach to evaluate smartphone data.

This section briefly reviews the formal definition of authentic smartphone data, the requirements to identify such data, as well as the smartphone data evaluation model.

2.1 Authentic Smartphone Data

Smartphones operate in an interconnected environment that involves several components responsible for the creation of smartphone data. These components are:

- End-user's interaction with and operation of the smartphone (End-user Behaviour).
- The current working and operational state of the smartphone (Smartphone Operational State).
- The behaviour and execution of installed applications (Smartphone Application Behaviour).
- The role of the mobile network as a delivery platform (External Environment).

Authentic smartphone data requires these four components to consistently operate as expected and remain unaffected. The importance of these components causes them to form critical pillars in maintaining the authenticity of smartphone data. Any affected component that operates irregularly directly impacts the authenticity of the smartphone data since an opportunity existed for the data to change. Digital forensic professionals must be able to evaluate these components to establish the authenticity of smartphone data.

2.2 Requirements for Authentic Smartphone Data

Confirming the four components operates as expected is possible by forming a collection of requirements. The requirements capture the expected operational behaviour of each component, allowing digital forensic professionals to assess the components. The outcomes produced by the requirements offer digital forensic professionals insight into the authenticity of the smartphone data.

A first attempt to identify requirements for evaluating smartphone data was performed by Pieterse et al. [2]. The authors presented seven theories of normality that captured the normal or expected behaviour of smartphone applications. Subsequent research [13] further extended the previously identified theories of normality by including additional requirements to also measure the operation of the smartphone and the impact of the environment external to the smartphone. The remainder of this section briefly describes the final requirements identified for authentic smartphone data.

The first component encapsulates the end-user and their use of the smartphone. Therefore, the requirements evaluate the expected operation of the smartphone and installed applications as operated by the end-user. The requirements belonging to the first component are (1.1) the assessment of smartphone application usage, (1.2) the operation of the smartphone with regards to rebooting and (1.3) eliminating the presence of anti-forensic applications.

The second component assesses the operational state of smartphones, which reflects changes made to the smartphone by the end-user. The focus of the requirements for this component is to evaluate (2.1) the smartphone state (whether the smartphone is rooted or jailbroken) and the (2.2) presence of known critical files. Critical files include any file that the digital forensic professional requires to establish the authenticity of the smartphone data.

The third component reviews the behaviour of installed smartphone applications. Assessing smartphone application behaviour requires digital forensic professionals to confirm that (3.1) internally stored data corresponds to user interface displayed data since data shown via the user interface can be cache data. The structure (i.e. database) responsible for storing persistent data must (3.2) follow a consistent pattern to store the data (records correctly ordered when listed using auto-incremented primary key and a date or timestamp fields). In addition, (3.3) changes to the file structure (file sizes) must occur consistently. An example of such change is SQLite databases that append new records in the Write-Ahead Log (WAL) file, causing an increase in the file size. Finally, (3.4) the ownership and file permissions assigned to the file structure must remain unchanged and constant.

The final component evaluates the environment external to the end-user and the associated smartphone. The external environment includes the smartphone data collected by other smartphones that directly communicated with the smartphone under investigation, as well as the records collected by the mobile network operator(s). Therefore, the requirements for this component focus on (4.1) confirming the persistent smartphone data stored on two or more smartphones corresponds by viewing the stored data, as well as (4.2) to the records collected by the mobile network operator(s).

Collectively, all of the presented requirements provide a comprehensive review of the smartphone data, as well as the components responsible for creating the data. The outcomes produced by the requirements not only describe the authenticity but also confirm whether opportunities existed for the data to be changed. However, the requirements

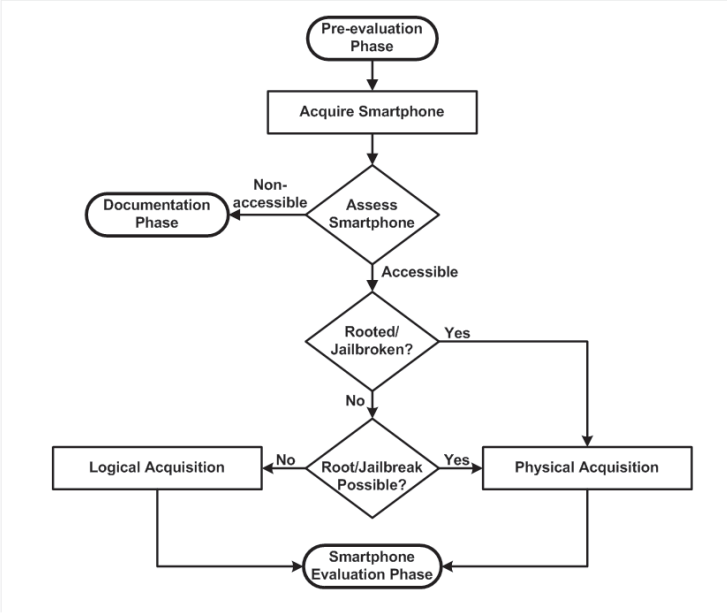

Figure 1. Pre-evaluation phase.

need formal arrangement and order to ensure optimal utilisation of the requirements by digital forensic professionals.

2.3 Smartphone Data Evaluation Model

The requirements identified equips digital forensic professionals with the necessary tools to evaluate smartphone data. There is, however, no structure or order to these requirements, which can impact their practical use when reviewing smartphone data. The smartphone data evaluation model structures the requirements and provides digital forensic professionals with a step-by-step guide for evaluating and reviewing smartphone data. The model consists of three phases: (i) pre-evaluation phase, (ii) smartphone evaluation phase and (iii) documentation phase.

The initial phase of the smartphone data evaluation model instructs digital forensic professionals to inspect the smartphone. Figure 1 presents the steps of the pre-evaluation phase. The results produced by the pre-evaluation phase describe the accessibility (locked or unlocked) and the current state (rooted or jailbroken) of the smartphone, as well as the most appropriate acquisition (logical or physical) technique to acquire the data. Logical acquisition retrieves a bit-by-bit copy of the logical file allocation storage area (file system partition), which includes directories

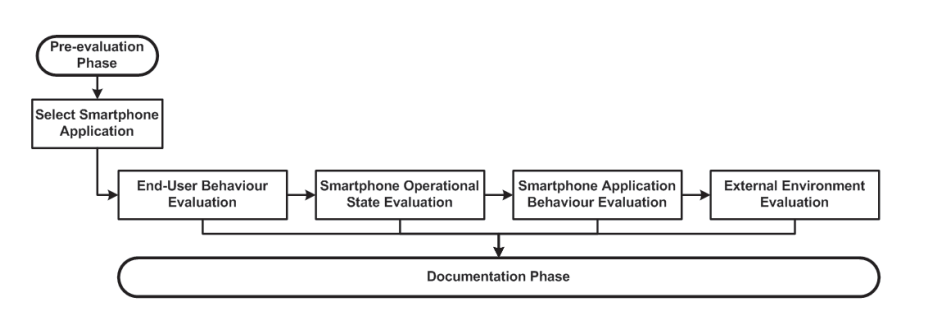

Figure 2. Smartphone evaluation phase.

and various file types [14, 15]. Physical acquisition obtains a bit-by-bit copy of the entire physical store (raw disk image) that also includes previously deleted or lost data [14, 15].

Following the pre-evaluation phase is the smartphone evaluation phase, which utilises the requirements identified in Section 2.2 to review the acquired smartphone data. Figure 2 illustrates the individual components of the smartphone evaluation phase, structured according to the components identified in Section 2.1. The first step of the smartphone evaluation phase instructs the digital forensic professional to select a single smartphone application to evaluate, which must reside on the smartphone. Once selected, the digital forensic professional must interpret and evaluate the collected smartphone data against the requirements of each component. The outcome of the smartphone evaluation phase is a collection of results that offers guidance to the digital forensic professional with regards to the authenticity of the evaluated smartphone data.

The documentation phase is the final phase of the smartphone data evaluation model, which collects and aggregates all the results produced during the previous phase. The collected results permit digital forensic professionals to make informed and well-weighted decisions regarding the evaluated smartphone data.

3. Classification Model

The smartphone data evaluation model, as described in the previous section, only stipulates how smartphone data must be evaluated without providing an outcome regarding the authenticity of the data. Further assistance can be provided to digital forensic professionals by formulat-

ing a classification model that classifies the authenticity of the evaluated smartphone data. Collectively, the requirements and smartphone data evaluation model presented in Section 2 provide the necessary foundation for establishing a classification model for smartphone data. The purpose of the classification model is to classify the authenticity of application-generated smartphone data residing on the smartphone. The output of the model is an authenticity classification that is an ordered pair of values describing the grade of authenticity and the completeness of the evaluation. The following sections describes the categorisation of the requirements, the calculation and representation of the authenticity score, measuring the of completeness of the evaluation, as well as visualising the final authenticity classification.

3.1 Categorisation of the Requirements

It is necessary to formulate a detailed mathematical equation that produces dependable results to consistently classify the authenticity of evaluated smartphone data. The basis of this mathematical equation is the requirements and smartphone data evaluation model presented in Section **??**. In total, eleven requirements were identified, and evaluation of each requirement occurs using one or more assessment points. The outcome of each assessment point is a ternary result `[yes/no/absent]`. A positive result `[yes]` confirms the requirement is met while a negative result `[no]` indicates the evaluated data contradicts the requirement. Should the data be unavailable or insufficient to evaluated the assessment point, an absent `[absent]` result is produced.

The impact of each result produced by the assessment points is, however, not equal since each assessment point evaluates different aspects of the authenticity of smartphone data. The categorisation of the assessment points into appropriate classes with a distinct focus will provide a more accurate evaluation of the authenticity. Stemming from the definition of authenticity, which describes data that preserves the same identify it had when first created and can be proven to have maintained its integrity over time, are two distinct classes. The first class (A) contains assessment points that confirm no opportunity existed to change the smartphone data. The second class (B) collects assessment points that evaluate the consistency of the various components responsible for creating the smartphone data, as well as the data itself. The purpose of class B assessment points is to evaluate the smartphone, the smartphone application and the application's associated data. Therefore, it is necessary to further categorise class B assessment points into the following subclasses:

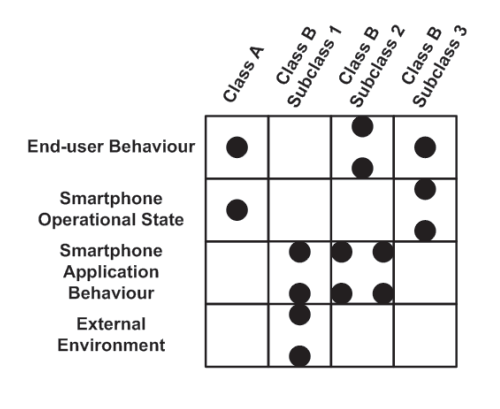

Figure 3. Categorisation of assessment points

- **Subclass 1 (B.1):** assessment points only evaluate the application's data.
- **Subclass 2 (B.2):** assessment points evaluate the behaviour of the application and the file structure used to store the data.
- **Subclass 3 (B.3):** assessment points evaluate the state of the smartphone.

Figure 3 categorise the available assessment points according to the classes established and the core components containing the requirements for authentic smartphone data. The categorisation of the assessment points according to classes A and B allows for a weighted calculation of the authenticity score.

3.2 Authenticity Score

Calculation of the authenticity score follows a weighted approach since the outcome of each assessment point impacts the authenticity of the smartphone data differently. The weighted calculation of the authenticity score relies, therefore, on the assignment of appropriate weights to each class. The weight assigned to each class reflects the impact the evaluated assessment point will have on the final authenticity score.

The previous section identified two distinct classes for assessment point categorisation. Since class A contains approximately 15% of the available assessment points (see Figure 3), a weight of 0.15 is assigned to the class. The weight assigned to class B is the remainder, which is 0.85 and represents a larger collection of assessment points. However, the assigned weight of class B must be further subdivided in order to

Table 1. Weight assignments of classes.

Class A	**Class B.1**	**Class B.2**	**Class B.3**
0.15	0.425	0.28	0.14

assign an appropriate weight for each individual subclass. The focus of subclass 1 assessment points is strictly aimed at the evaluation of the data of the smartphone application and the produced results will, therefore, have a significant influence the outcome of the authenticity score. The importance of the results produced by these assessment points necessitates a larger weight to be assigned to subclass 1. The mean of the weight originally attributed to class B is assigned as the weight of subclass 1. Assessment points belonging to subclass 2 focus on evaluating the behaviour of the smartphone application but excludes the application's data. The results produced by evaluating the behaviour of the smartphone application has a lesser influence on the calculated authenticity than the evaluation of the data. Assigned as the weight of subclass 2 is the mean of two-thirds of the original weight attributed to class B. Finally, assessment points of subclass 3 focus only on the smartphone. Since these assessment points do not directly address the smartphone application or related data, the produced results will have a minimal impact on the authenticity score. Therefore, subclass 3 receives a weight that is the mean of one-third of the original class B weight. Table 1 presents the weight for each class (w_c), where c represents the class identifier.

Calculation of the score for class A occurs using equation 1. The assessment points evaluated per class produce a collection of positive or negative results. However, the acquisition technique followed to acquire the data (see Section 2.3) can impact the ability to assess all available assessment points. Therefore, the collection of positive (pos_c) results are divided by the number of assessment points evaluated per class (n_c), which is then weighed using the assigned weight (w_c) as shown in Table 1. The score for class B is calculated using equation 2 and is the sum of the individual scores of the subclasses. Equation 3 calculates the final authenticity score (A_s), which is the sum of the scores calculated for classes A and B.

$$S_A = w_c \frac{pos_c}{n_c} \tag{1}$$

$$S_B = \sum_{c=1}^{3} w_c \frac{pos_c}{n_c} \tag{2}$$

$$A_s = \sum_{c=A}^{B} S_c \tag{3}$$

Currently, the presented authenticity score is merely a percentage and lacks context or description. It is necessary to further describe the authenticity score by assigning an appropriate grade.

3.3 Authentic Grading Scale

The authenticity score, produced by the mathematical equations introduced during the previous section, presents the authenticity of the evaluated smartphone data as a percentage. The percentage, alone, is inadequate and requires further description and categorisation to better reflect the classified authenticity of the smartphone data. The categorisation of the authenticity score requires additional interpretation of the evaluated assessment points and all possible outcomes. Both the number of assessment points evaluated and the possible outcomes factor significantly into the categorisation of the authenticity score. Therefore, it is first necessary to confirm the assessment points evaluated and calculate all possible outcomes relating to the evaluation of these assessment points. The result is a collection of outcomes that follows a bell shaped curve or normal distribution. The normal distribution presents two clusters of potential outcomes. The first cluster (below the mean of the normal distribution) present the outcomes of evaluated assessment points that mostly produced negative results. It is possible to further group these outcomes as follows:

- Outcomes of evaluated assessment points is negative (authenticity unsatisfactory).
- Outcomes of assessment points produced more negative results that outweighed the positive results (authenticity low).

The second cluster of outcomes (above the mean of the normal distribution) represent the opposite where the outcomes of the evaluated assessment points mostly produced positive results. It is also possible to further group these outcomes as follows:

- Outcomes of assessment points produced more positive results that outweighed the negative results (authenticity moderate).

Table 2. Authentic grading scale for evaluated smartphone data.

Grade	Description
Unsatisfactory	Fails to meet most of the requirements.
Low	Meets some of the requirements.
Moderate	Mostly meets requirements captured in subclasses 2 and 3.
High	Mostly meets requirements captured in subclasses 1 and 2.

- Outcomes of evaluated assessment points is positive (authenticity high).

The classification model, therefore, presents four distinct grades that can be used to construct the authentic grading scale (see Table 2). To assign a grade to the final authenticity score, it necessary to divide the normal distribution of all outcomes into quartiles. The lower quartile distinguishes between the unsatisfactory and low authentic grading, the middle quartile separates the low and moderate authentic grading and the upper quartile distinguishes the high authentic grading from the moderate authentic grading.

The quartiles make it is possible to construct the authentic grading scale that provides context and better describes the classified authenticity. The quartile values provide the boundaries between the distinct grades of authenticity. The authenticity score is then plotted on the scale to determine the authentic grading of the evaluated smartphone data. This constant and formal measurement of smartphone data ensures that digital forensic professionals can conclusively establish the authenticity of smartphone data and also easily comprehend the grade of authenticity among one another.

3.4 Completeness

The calculation of the authenticity score and the construction of the authentic grading scale directly depends on the collection of assessment points evaluated. Influencing the availability of these assessment points is the acquisition technique used to acquire the smartphone data. The completeness score (C_S) represents the relationship between the evaluated and all of the available assessment points per component (see Figure 3) and is established using equation 4. The completeness score allows digital forensic professionals to present the authenticity score of the evaluated smartphone data with certain confidence. Therefore, the calculated completeness score compliments the authenticity grading.

$$C_s = \sum_{i=1}^{4}(\frac{a_i}{t_i})(0.25) \tag{4}$$

For each component (see Section 2.1), the evaluated assessment points (a_i) are counted and divided by the total assessment points (t_i) available for that component. The final completeness score is a weighted score calculated using 25% weight measurement per component. The weighted score ensures equal importance among the components. A more substantial collection of assessment points evaluated presents a more thorough and complete classification of the authenticity of the smartphone data. The availability of fewer assessment points highlights a more partial evaluation of the smartphone data, lowering the confidence associated with the classification of the authenticity of the smartphone data.

3.5 Authenticity Classification

The calculated authenticity (A_S) and completeness (C_S) scores are the key results produced by the classification model. These scores form an ordered pair of values that represents the final authenticity classification (A_C) of the evaluated smartphone data (see Equation 5).

$$A_C =< A_S; C_S > \tag{5}$$

Visual representation of the final authenticity classification occurs using the authenticity classification graph shown in Figure 4. The authenticity classification graph follows a two-dimensional structure to depict both the grade of authenticity and the completeness of the evaluation. The x-axis represents the authentic grading scale, and the vertical lines divide the available space into four quartiles to portray the four grades of authenticity. The y-axis represents the completeness scale, and the single horizontal line distinguishes between higher and lower confidence of classification. Finally, the drawn square illustrates and confirms the authenticity classification of the evaluated smartphone data.

4. Smartphone Application Data Authenticity Classifier (SADAC)

SADAC is a proof of concept digital forensic tool that automates the mathematical equations provided by the classification model. Although digital forensic professionals can manually complete the provided equations, human error can impact the final classification of the authenticity. The remainder of this section focuses on the functional requirements and

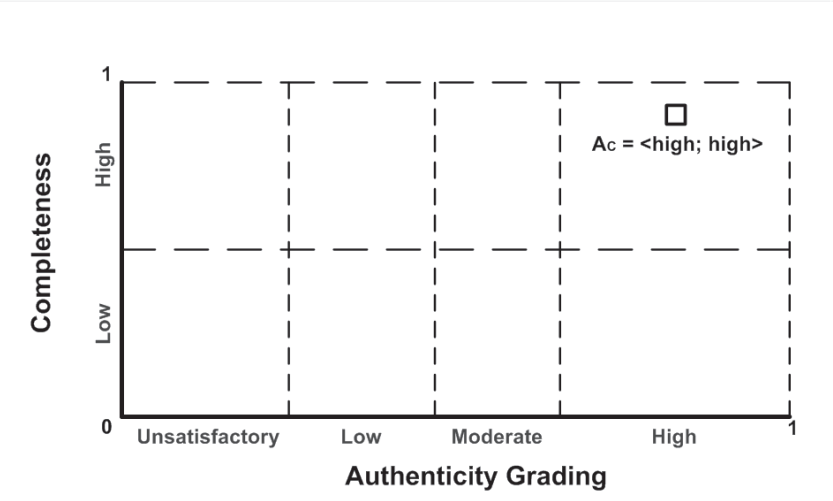

Figure 4. Authenticity classification graph.

interface design of the SADAC tool, as well as a practical experiment involving manipulated smartphone data.

4.1 Tool

The purpose of the SADAC tool is to accurately calculate and present the authenticity classification of the evaluated smartphone data. Therefore, the primary objective of the SADAC tool is to quicken, simplify and ensure the accuracy of the calculated authenticity classification. The SADAC tool supports the evaluation of all assessment points of all requirements and collects the outcome of each assessment point's ternary result `[yes/no/absent]`. Collectively, these results are then used to calculate the authenticity and completeness scores using the provided equations.

Figure 5 captures the structural ordering and layout of the SADAC user interface. The central viewing area of the SADAC tool consists of functional tabs, three interactive buttons and a canvas to draw the authenticity classification graph. Each tab represents a component of authentic smartphone data and captures all assessment points belonging to the requirements for each component. Representation of the ternary result `[yes/no/absent]` for each assessment point is achieved using radio buttons, which enforces the selection of only a single option. The "Calculate" button collects the results of all evaluated assessment points and computes the authenticity classification using the provided equations.

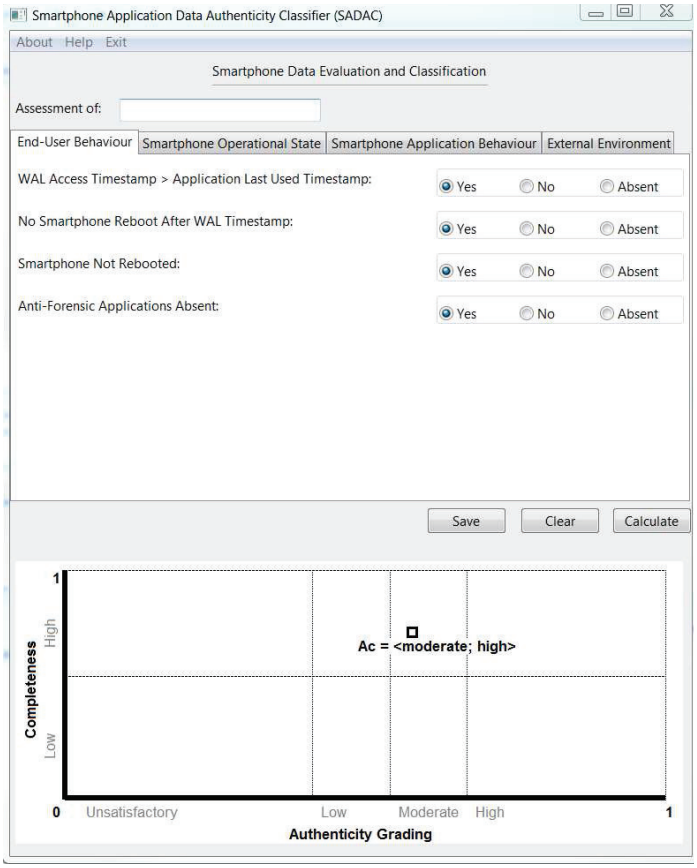

Figure 5. SADAC interface design.

The authenticity is presented using the authenticity classification graph in the canvas panel below the buttons.

The simple and minimalistic design of the user interface for the SADAC tool allows for easy comprehension and effective operation of the available functions. It is only necessary for digital forensic professionals to provide the SADAC tool with the required input as the remainder of the process is entirely automated. It is, however, important to note that the SADAC tool is developed to compliment existing digital forensic toolkits.

4.2 Practical Experiment

The newly introduced classification model and developed SADAC tool allow for quick and efficient evaluation of the authenticity of smartphone

data. It is possible to further validate the classification model by conducting a practical experiment. The experiment relies on the generic process for smartphone data manipulation [7] that describes the stages to follow to alter smartphone data. The four stages for smartphone data manipulation are as follows:

- **Phase 1**: ensures the selected smartphone is accessible by confirming the smartphone is either rooted (Android) or jailbroken (iOS).
- **Phase 2**: requires the selection of the application and identifying the location of the file(s), such as a SQLite database, storing the smartphone data.
- **Phase 3**: identify the most appropriate approach to access the smartphone data: Direct or Off-device. The direct approach performs the manipulation of the smartphone data directly on the smartphone and relies on the presence of a program or utility to access the file(s). The off-device approach requires the transferral of the file(s) to and from a connected computer with the required program or utility installed to perform the manipulation.
- **Phase 4**: requires a manual reboot of the smartphone.

The experiment involves an iPhone 7 and the creation of a new but fabricated text message. The outlined generic process for smartphone data manipulation allows for the creation of the fabricated text message, which forms part of iPhone's default messaging application. The following steps summarise the creation of the fabricated text message:

1 Jailbreak the iPhone 7 (using the `extra_recipe + yaluX` application).

2 Pinpoint the storage structure (SQLite database) of iPhone's default messaging application (`/private/var/mobile/Library/SMS/sms.db`).

3 Follow the direct approach and insert a fabricated text message into the SQLite database using the pre-installed `sqlite3` command-line utility.

4 Reboot the iPhone 7 to complete the manipulation process and ensure the changes reflect on the smartphone.

Completing the manipulation of smartphone data has inherent side-effects that creates various traces. Table 3 lists the traces specific to

Table 3. Traces created by the experiment.

Trace No.	Created Trace
T_1	Automatic installation of the Cydia application.
T_2	Unavailability of OTA updates.
T_3	Discrepancy between WAL file and application usage timestamps.
T_4	Usage of the `sqlite3` program.
T_5	Presence of a clean WAL file.
T_6	The creation of entry in the reboot log file.
T_7	Discrepancy in the mobile network provider records

this experiment. Jailbreaking the iPhone 7 causes the automatic installation of the Cydia application and prevents the availability of OTA updates. Again gaining access to the persistent data stored in the SQLite database following the direct approach but without accessing the application causes a discrepancy between the last modification timestamp of the SQLite database and the last usage timestamp of the application. The direct approach relies on the use of the `sqlite3` program to acquire access to the persistent data, which causes a change to the last access timestamp associated with the program. This timestamp will also closely follow the last modification timestamp of the SQLite database. Accessing the SQLite database to manipulate the record will cause an immediate checkpoint to occur. Therefore, after closing the SQLite database, a clean and empty WAL is present on the iPhone 7. Finally, rebooting the iPhone 7 causes the creation of a new entry in the `/var/mobile/logs/lockdownd.log` reboot log. Although not present on the iPhone 7, creating the fabricated text message also causes discrepancies in the records captured by mobile network providers.

Using the traces collected in Table **??** as input makes it possible to evaluate the authenticity of the smartphone data using the SADAC tool. The outcome of the authenticity grading is expected to be either "low" or "unsatisfactory" due to the changes made to the iPhone 7 to include the fabricated text message. Further expected is a "high" completeness value since all assessment points were evaluated.

Figure 6 presents the authenticity classification of the evaluated smartphone data. The calculated authenticity classification confirms the assignment of an "low" authenticity grading. Furthermore, the authenticity classification also confirms a "high" completeness value, which is expected since the assessment points of all requirements were evaluated. The assigned authenticity classification aligns with the predicted outcome and confirms that the manipulation does indeed influence the au-

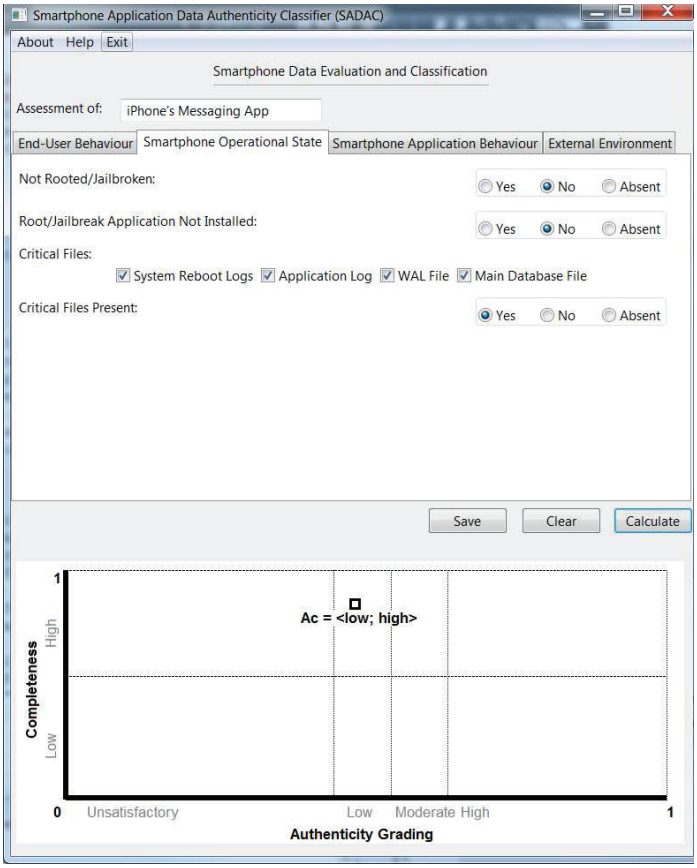

Figure 6. Outcome of the practical experiment.

thenticity of the data. The assignment of the authenticity classification concludes the evaluation of the iPhone 7 smartphone data.

5. Conclusions

Captured smartphone data provides digital forensic professionals with a well-defined snapshot of end-user events. The value of smartphone data as digital evidence emphasises the importance of confirming the authenticity of the data since such data can be compromised by anti-forensics, malware or users with malicious intent. The available smartphone data evaluation model describes how to review smartphone data but excludes any form of classification of the authenticity of the data. Therefore, the paper addressed this shortcoming by introducing a new classification model that serves to classify evaluated smartphone data using an ordered

pair of values. The authenticity classification describes the authenticity of the smartphone data using an appropriate grade and completeness value. The developed SADAC tool streamlines both the evaluation and classification of smartphone data. An experiment involving the fabrication of smartphone data demonstrated that the classification model provides significant investigatory assistance to digital forensic professionals. Collectively, the smartphone data evaluation and classification models enable digital forensic professionals to pinpoint and remove unreliable smartphone data before arriving at conclusions.

Demonstrated in this paper was the evaluation and classification of a single application's smartphone data. Future work can extend this research to focus on multiple smartphone applications and the ability to identify patterns among the smartphone data. Identification of particular patterns can either further promote or oppose the authenticity of a certain smartphone application's data.

References

[1] G. Cecere, N. Corrocher and R.D. Battaglia, Innovation and competition in the smartphone industry: Is there a dominant design?, *Telecommunications Policy*, vol. 39 no. 3-4, pp. 162–175, 2015.

[2] H. Pieterse, M. Olivier and R. van Heerden, Evaluating the Authenticity of Smartphone Evidence, *Advances in Digital Forensics XIII*, G. Peterson and S. Shenoi (Eds.), Springer, pp. 41–61, 2017.

[3] P. Albano, A. Castiglione, G. Cattaneo, G. De Maio and A. De Santis, On the construction of a false alibi on the Android OS. *Third International Conference on Intelligent Networking and Collaborative Systems (INCoS)*, pp. 685–690, 2011.

[4] M. Hannon, An increasingly important requirement: Authentication of digital evidence, *Journal of the Missouri Bar*, vol. 70, no. 6, pp. 314–323, 2014.

[5] R. Harris Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem, *Digital Investigation*, vol. 3, pp. 44–49, 2006.

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

[7] H. Pieterse, M. Olivier and R. van Heerden, Detecting Manipulated Smartphone Data on Android and iOS Devices, *Communications in Computer and Information Science*, H. Venter, M. Loock, M. Coetzee, M. Eloff and J. Eloff (Eds.), Springer, pp. 89–103, 2018.

[8] B.L. Schatz, Digital evidence: Representation and assurance, Doctoral Dissertation, Queensland University of Technology, Brisbane, Queensland, Australia, 2007.

[9] E. Casey, *Digital evidence and computer crime: Forensic science, computers, and the Internet*, Academic press, Cambridge, Massachusetts, USA, 2011.

[10] F. Cohen, *Digital Forensic Evidence Examination*, Fred Cohen & Associates, Livermore, CA, USA, 2009.

[11] L. Duranti, From digital diplomatics to digital records forensics, *Archivaria, The Journal of the Association of Canadian Archivists*, vol. 68, pp. 39–66, 2009.

[12] M. Losavio, Non-technical manipulation of digital data, *Advances in Digital Forensics*, M. Pollitt and S. Shenoi (Eds.), Springer, Boston, MA, USA, vol. 194, pp. 51–63, 2005.

[13] H. Pieterse, M. Olivier and R. van Heerden, Smartphone data evaluation model: Identifying authentic smartphone data, *Digital Investigation*, vol. 24, pp. 11–24, 2018.

[14] W. Jansen and R. Ayers, Guidelines on cell phone forensics, NIST Special Publication 800–101, National Institute of Standards and Technology, Gaithersburg, Maryland, USA, 2007.

[15] M. Bader and I. Baggili, iPhone 3GS forensics: Logical analysis using Apple iTunes backup utility, *Small Scale Digital Forensics Journal*, vol. 4 no. 1, pp. 1–15, 2010.