Classifying the Authenticity of Evaluated Smartphone Data

Heloise Pieterse, Martin Olivier, Renier Van Heerden

Chapter 3

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 smartphones in daily activities create large quantities of smartphone data. This 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 intentional or accidental alterations by users or installed applications. It is, therefore, essential to establish the authenticity of smartphone data before submitting it as evidence. Previous research has formulated a smartphone data evaluation model, which provides a methodical 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 about the authenticity of the data.

This chapter proposes a new classification model that provides a grade of authenticity for evaluated smartphone data along with a measure of the completeness of the evaluation. Experimental results confirm the effectiveness of the proposed model in classifying the authenticity of smartphone data.

Keywords: Mobile device forensics, smartphone data, authenticity

1. Introduction

The competitive nature of the global smartphone market [4] stimulates continuous advancements in smartphone technology. The advancements enable smartphone models to support different operating systems and permit the installation of diverse third-party applications. The current capabilities of smartphones coupled with their widespread use in daily activities lead to rich collections of data. Smartphone data "includes any data of probative value that is generated by an application or transferred to the smartphone by the end-user" [12]. Generally, smartphone data

describes events that occurred on the smartphone and the associated timestamps support the chronological ordering of the events [1]. As a result, smartphone data constitutes valuable digital evidence in civil and criminal investigations.

Smartphone data is, however, susceptible to modification [7]. Changes to smartphone data can occur during the execution of incorrect or error-prone applications or deployed malware. Furthermore, users with malicious intent can alter smartphone data intentionally. Intentional changes to smartphone data are commonly referred to as anti-forensics, which "compromise[s] the availability or usefulness of evidence to the forensic process" [8]. While several studies have successfully demonstrated the manipulation, fabrication and alteration of smartphone data [11, 14], unknown or unexpected changes to smartphone data that go undetected can lead to erroneous conclusions in investigations. Therefore, it is essential for digital forensic professionals to establish the authenticity of smartphone data before formulating any conclusions [15]. Authenticity 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 [3, 5, 6, 10].

Establishing the authenticity of smartphone data requires a good understanding of the smartphone operating environment and the key components that are responsible for creating smartphone data. These components include the smartphone applications that generate data, operation of the smartphone by the end-user and the impact of the immediate surroundings.

Pieterse et al. [13] formally defined the term "authenticity" with regard to smartphone data and used the definition to articulate several requirements for evaluating the authenticity of the data. These requirements were subsequently employed to construct a smartphone data evaluation model that provides digital forensic professionals with a structured approach for evaluating the authenticity of smartphone data. However, the data evaluation model only stipulates how to evaluate smartphone data – it does not provide a formal classification of the authenticity of the evaluated data. Meanwhile, classification scales for digital evidence, such as Casey's certainty scale or degrees of likelihood (almost definitely, most probably, probably, very possible or possibly) [3], have been proposed for specifying the certainty of conclusions. A formal and consistent methodology for classifying the authenticity of smartphone data would provide further support to the certainty of investigative conclusions.

This chapter introduces a new classification model for smartphone data, which is constructed using the smartphone data evaluation model

and the requirements for evaluating the authenticity of smartphone data. The classification model assesses smartphone data using an ordered pair of values. The first value corresponds to a grade of authenticity while the second value describes the completeness of the evaluation. This classification enables digital forensic professionals to present the authenticity of evaluated smartphone data with confidence. Experiments involving the manipulation of iPhone 7 data confirm the effectiveness of the classification model in assessing the authenticity of smartphone data.

2. Background

A detailed analysis of smartphone data offers contextual information about the end-user as well as the activities performed with the smartphone. Therefore, smartphone data can constitute valuable digital evidence in civil and criminal investigations. The authenticity of smartphone data is of great importance to ensuring that digital forensic professionals draw correct and accurate conclusions based on the data. In order to formulate proper conclusions, digital forensic professionals must be able to review smartphone data and to evaluate its authenticity.

The smartphone data evaluation model of Pieterse et al. [13] offers a methodical approach for evaluating smartphone data. This section briefly reviews the formal definition of authentic smartphone data, the requirements for identifying smartphone data and the smartphone data evaluation model.

2.1 Authentic Smartphone Data

Smartphones operate in interconnected environments where several components are responsible for creating smartphone data. These components are:

- **End-User Behavior:** End-user operation of and interactions with a smartphone.
- **Smartphone Operation:** The working and operational states of a smartphone.
- **Smartphone Application Behavior:** The behavior and execution of installed applications on a smartphone.
- **External Environment:** The roles of mobile networks as delivery platforms.

Authentic smartphone data requires the four components to consistently operate as expected and to remain unaffected. The importance

of these components renders them critical to maintaining data authenticity. An affected component that operates irregularly directly impacts data authenticity because an opportunity exists for the data to change. Digital forensic professionals must evaluate all the components in order to establish the authenticity of smartphone data.

2.2 Requirements for Authentic Data

A set of requirements is needed to confirm that the four components operate as expected. The requirements should capture the expected operational behavior of each component, enabling digital forensic professionals to assess the components. The outcomes produced by the requirements would offer digital forensic professionals insights into the authenticity of smartphone data.

Pieterse et al. [12] were the first researchers to identify requirements for evaluating smartphone data. They presented seven theories of normality that capture the normal or expected behavior of smartphone applications. Subsequent research [13] extended the theories of normality by including additional requirements that assess the operation of smartphones and the impacts of the environments external to the smartphones. The remainder of this section discusses the final requirements identified for authentic smartphone data.

The first component covers the end-user and his/her use of the smartphone. Therefore, the requirements evaluate the expected operation of the smartphone and the installed applications as operated by the end-user. The requirements related to the first component are: (1.1) assessing smartphone application usage; (1.2) assessing the operation of the smartphone with regard to rebooting; and (1.3) assessing the presence of anti-forensic applications.

The second component covers the operational state of the smartphone, which reflects the changes made to the smartphone by the end-user. The requirements are: (2.1) assessing the smartphone state (i.e., whether or not the smartphone is rooted or jailbroken); and (2.2) assessing the essence of known critical files. A critical file is one that is used by a digital forensic professional to establish the authenticity of smartphone data.

The third component covers the behavior of the installed smartphone applications. One requirement related to smartphone application behavior is: (3.1) confirming that the internally-stored data corresponds to the data displayed on the user interface (because the data shown on the user interface could be cached data). Another requirement is: (3.2) confirming that the structure (i.e., database) responsible for storing persistent

data follows a consistent pattern in storing data (i.e., records are correctly ordered when listed using an auto-incremented primary key and a date or timestamp). In addition: (3.3) confirming that all changes to the file structure (file sizes) occur consistently. An example is a SQLite database that appends new records in a write-ahead log (WAL), which causes the file size to increase. The last requirement is: (3.4) confirming that the ownership and file permissions assigned to the file structure remains unchanged.

The fourth component covers the environment external to the end-user and smartphone. The external environment includes smartphone data collected by other smartphones that directly communicated with the smartphone under investigation, as well as the records collected by mobile network operators. Therefore, the requirements for this component are: (4.1) confirming that the persistent smartphone data stored on two or more smartphones corresponds to the viewed data; and (4.2) confirming that the persistent smartphone data corresponds to the records collected by mobile network operators.

The requirements collectively enable comprehensive reviews of smartphone data as well as the components responsible for creating the data. The outcomes produced by the requirements describe the authenticity of the data and confirm whether or not opportunities existed for the data to be modified. However, the requirements need to be ordered in a formal manner to ensure their optimal use by digital forensic professionals.

2.3 Smartphone Data Evaluation Model

The requirements discussed above provide digital forensic professionals with a mechanism for evaluating smartphone data. However, the absence of structure or order to these requirements can impact their use in investigations. Consequently, the proposed smartphone data evaluation model structures the requirements to provide digital forensic professionals with a step-by-step guide for evaluating and reviewing smartphone data.

The smartphone data evaluation model has three phases: (i) pre-evaluation phase; (ii) evaluation phase; and (iii) documentation phase.

- **Pre-Evaluation Phase:** In this phase, a digital forensic professional performs an inspection of the smartphone. Figure 1 presents the steps involved in this phase. The results produced by the phase describe the smartphone accessibility (i.e., locked or unlocked) and current smartphone state (i.e., rooted or jailbroken), along with the most appropriate data acquisition technique (i.e., logical or physical). Logical acquisition retrieves a bit-for-bit copy of the logical

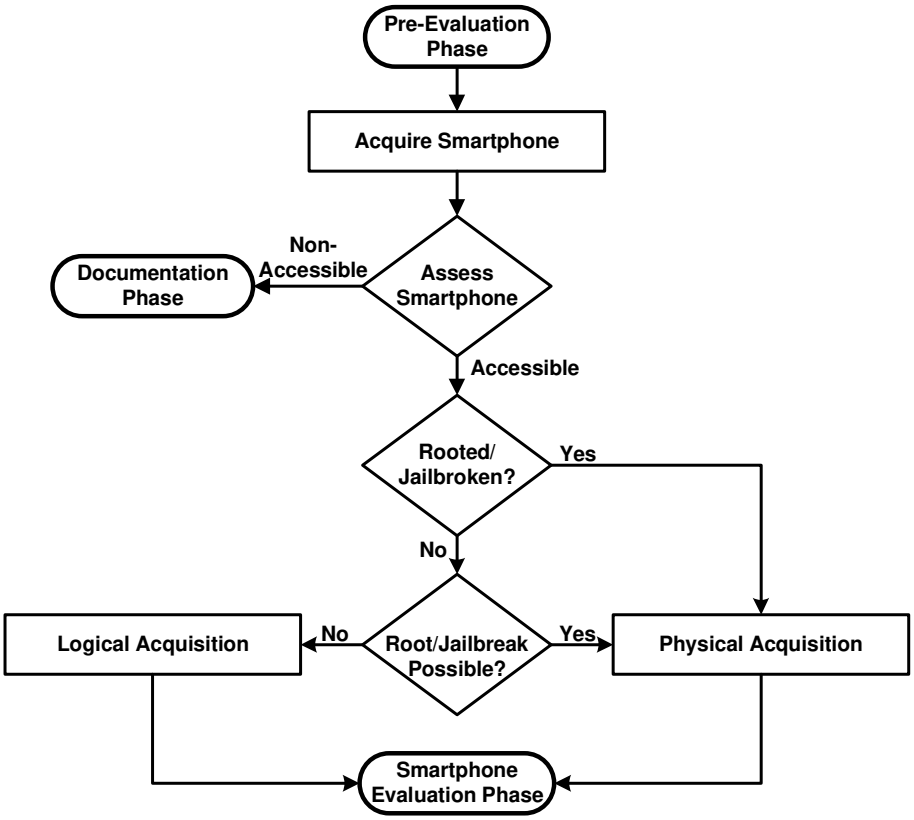

Figure 1. Pre-evaluation phase.

file allocation storage area (filesystem partition), which includes directories and files of various types [2, 9]. Physical acquisition obtains a bit-for-bit copy of the entire physical store (raw disk image), which includes deleted and lost data [2, 9].

- **Evaluation Phase:** The evaluation phase, which follows the pre-evaluation phase, engages the requirements identified in Section 2.2 to review the acquired smartphone data. Figure 2 shows the steps involved in the evaluation phase, which are structured according to the four components identified in Section 2.1.

  In the first step of the evaluation phase, a digital forensic professional selects a single smartphone application to be evaluated; this application must reside on the smartphone. After the application is selected, the digital forensic professional interprets and evaluates the collected smartphone data against the requirements of each of

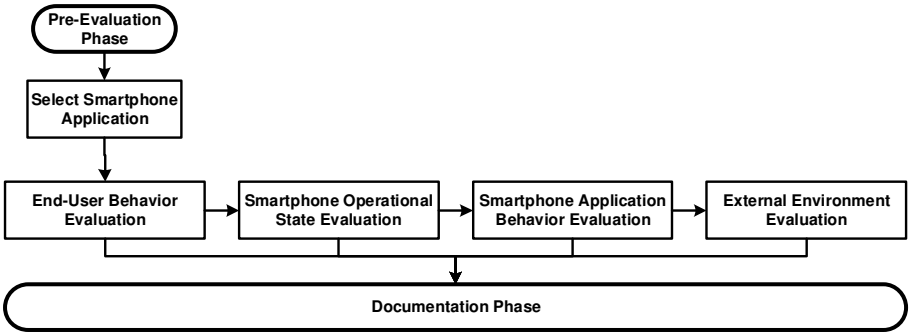

Figure 2. Evaluation phase.

the four components. The outcome of the evaluation phase is a collection of results that offers guidance to the digital forensic professional about the authenticity of the evaluated smartphone data.

- **Documentation Phase:** The final documentation phase of the smartphone data evaluation model involves the collection and aggregation of all the results produced during the evaluation phase. The results enable a digital forensic professional to make informed decisions pertaining to the evaluated smartphone data.

3. Classification Model

The smartphone data evaluation model only stipulates how the data is to be evaluated without providing an outcome regarding the authenticity of the data. Further assistance can be provided to a digital forensic professional by formulating a classification model that assesses the authenticity of the evaluated smartphone data. Collectively, the requirements and smartphone data evaluation model presented in Section 2 provide a foundation for establishing a classification model for smartphone data. The purpose of the classification model is to formally assess the authenticity of application-generated smartphone data residing on a smartphone. The output of the model is an authenticity classification – an ordered pair of values that expresses the grade of authenticity and the completeness of the evaluation.

The following sections describe the categorization of the requirements, the computation and representation of an authenticity score, the measurement of the completeness of an evaluation, along with the visualization of the final authenticity classification.

3.1 Categorization of the Requirements

Mathematical equations are required to consistently classify the authenticity of evaluated smartphone data. The equations must embody the requirements and smartphone data evaluation model presented in Section 2. In total, eleven requirements were identified and the evaluation of each requirement involves one or more assessment points. Each assessment point has one of three outcomes: (i) yes; (ii); no; or (iii) absent. A positive result of yes confirms that the requirement is met. A negative result of no indicates that the evaluated data does not meet the requirement. An absent result is assigned when the data is unavailable or insufficient.

The results produced by the assessment points are not equally important because each assessment point evaluates different aspects of the authenticity of smartphone data. The categorization of the assessment points into classes, each with a distinct focus, enables a more accurate evaluation of data authenticity.

Two classes are defined based on the notion of smartphone data authenticity considered in this work. Class A contains assessment points that confirm that no opportunity existed to change the smartphone data. Class B comprises assessment points that evaluate the consistency of the components responsible for creating smartphone data, as well as the consistency of the data itself. The assessment points in Class B evaluate the smartphone, smartphone applications and data associated with the applications. Therefore, Class B assessment points are placed in the following three subclasses:

- **Subclass B.1:** Assessment points that only evaluate application data.
- **Subclass B.2:** Assessment points that evaluate application behavior and the file structure used to store data.
- **Subclass B.3:** Assessment points that evaluate the smartphone state.

Figure 3 categorizes the assessment points according to the established classes and the core components involved in the requirements for authentic smartphone data. The categorization of the assessment points into Class A and Class B allows for weighted calculations of the authenticity scores.

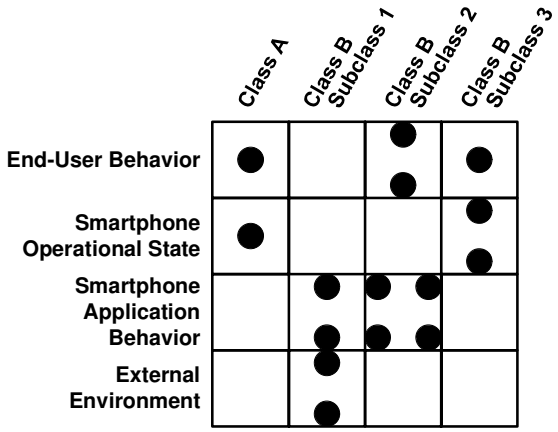

Figure 3. Categorization of assessment points.

3.2 Authenticity Score

The computation of the authenticity score is weighted because the outcome of each assessment point impacts the authenticity of the smartphone data differently. The weight assigned to each class should reflect the impacts that the constituent assessment points have on the final authenticity score.

Since Class A contains approximately 15% of the assessment points (Figure 3), a weight of 0.15 is assigned to the class. Class B, which contains the remaining assessment points, is assigned a weight of 0.85.

The Class B weight is subdivided to assign appropriate weights to its constituent subclasses. Subclass B.1 assessment points focus strictly on the evaluation of smartphone application data, which has a significant influence on the authenticity score. Since the Subclass B.1 assessment points are important, the subclass is assigned a weight of 0.425, one-half of the total weight of its parent Class B (0.85).

Assessment points in Subclass B.2 focus on the behavior of the smartphone application, but exclude the application data. Since these assessment points have less influence on the authenticity score than the Subclass B.1 assessment points that focus on data, Subclass B.2 is assigned a weight of 0.28, two-thirds of the remaining weight of Class B, which corresponds to one-third of the total weight of Class B ($1/3 \times 0.85 = 0.28$).

The assessment points in Subclass B.3 focus only on the smartphone and do not directly address smartphone applications and related data; thus, they have a limited influence on the authenticity score. Therefore,

Table 1. Weight assignments.

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

Subclass B.3 is assigned the remaining weight of 0.14, which corresponds to one-sixth of the total Class B weight ($1/6 \times 0.85 = 0.14$). Table 1 shows the assignments of weights to the classes and subclasses.

Because the outcome of each assessment point is a yes (= +1), no (= –1) or absent (= 0), positive or negative results are produced. However, the acquisition technique used to obtain the data can impact the ability to assess all the assessment points. Therefore, for each class c, the collection of positive results pos_c are divided by the number of assessment points n_c evaluated per class. The result is then weighted using the class weight w_c shown in Table 1.

Thus, the authentication score S_A for Class A is computed as:

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

The authentication score S_B for Class B is computed as the sum of the individual scores of its subclasses:

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

The final authenticity score A_s is computed as the sum of the scores computed for Classes A and B:

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

3.3 Authenticity Grading Scale

The authenticity score, as computed above, expresses the authenticity of the evaluated smartphone data as a percentage. The percentage value alone is inadequate – further description and categorization are required to better reflect the authenticity of smartphone data. Specifically, the categorization requires additional interpretation of the evaluated assessment points and all the possible outcomes. Since the number of assessment points evaluated and the possible outcomes factor significantly in the categorization of the authenticity score, it is necessary to confirm

Table 2. Authenticity grading scale for smartphone data.

Grade	Description
Unsatisfactory	Fails to meet most of the requirements.
Low	Meets some of the requirements.
Moderate	Meets most of the requirements in Subclasses B.2 and B.3.
High	Meets most of the requirements in Subclasses B.1 and B.2.

the evaluations of the assessment points and compute all the possible outcomes relating to the evaluations of these assessment points. The result is a set of outcomes that has a normal distribution.

The normal distribution presents two clusters of potential outcomes. The first cluster (below the mean of the normal distribution) corresponds to the outcomes of the evaluated assessment points that mostly produce negative results. The outcomes are further grouped as follows:

- **Unsatisfactory Authenticity:** The outcomes of the evaluated assessment points produce only negative results.
- **Low Authenticity:** The outcomes of the evaluated assessment points produce negative results that outweigh the positive results.

The second cluster of outcomes (above the mean of the normal distribution) corresponds to the outcomes of the evaluated assessment points that mostly produce positive results. The outcomes are further grouped as follows:

- **Moderate Authenticity:** The outcomes of the evaluated assessment points produce positive results that outweigh the negative results.
- **High Authenticity:** The outcomes of the evaluated assessment points produce only positive results.

Table 2 shows the four grades in the authenticity grading scale. In order to assign a grade to the final authenticity score, it necessary to divide the normal distribution of all the outcomes into quartiles. The lower quartile distinguishes between the unsatisfactory and low authenticity grades, the middle quartile distinguishes between the low and moderate authenticity grades, and the upper quartile distinguishes between the moderate and high authenticity grades.

The quartiles enable the authenticity grading scale to provide context and better describe smartphone data authenticity. The quartiles create

the boundaries between distinct grades of authenticity. The authenticity score is then plotted on the scale to determine the authenticity grade of the evaluated smartphone data. The consistent and formal measurement of smartphone data ensures that a digital forensic professional can conclusively establish the authenticity of smartphone data and also comprehend different grades of authenticity.

3.4 Completeness

The computation of authenticity scores and construction of the authenticity grading scale depend on the collection of assessment points that are evaluated. The specific acquisition technique used to obtain smartphone data strongly influences the availability of assessment points. A completeness score is required to express the number of the assessment points evaluated per component with respect to the number of available assessment points per component. This score would enable a digital forensic professional to present the completeness of the smartphone data evaluation with confidence, thereby complementing the authenticity grade.

The completeness score C_s is given by:

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

where a_i is an evaluated assessment point and t_i is the total number of assessment points available for the component. For each component specified in Section 2.1, the evaluated assessment points a_i are counted and divided by the total assessment points t_i, yielding a weighted score computed using a 25% weight measurement per component. The weighted score ensures that each component is equally important. Evaluating a larger collection of assessment points would yield a more thorough classification of the authenticity of smartphone data. The availability of fewer assessment points would yield a partial evaluation, reducing the confidence in the authenticity of smartphone data.

3.5 Authenticity Classification

The authenticity A_S and completeness C_S scores are the key results produced by the classification model. The final authenticity classification A_C of the evaluated smartphone data is an ordered pair of the two individual scores:

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

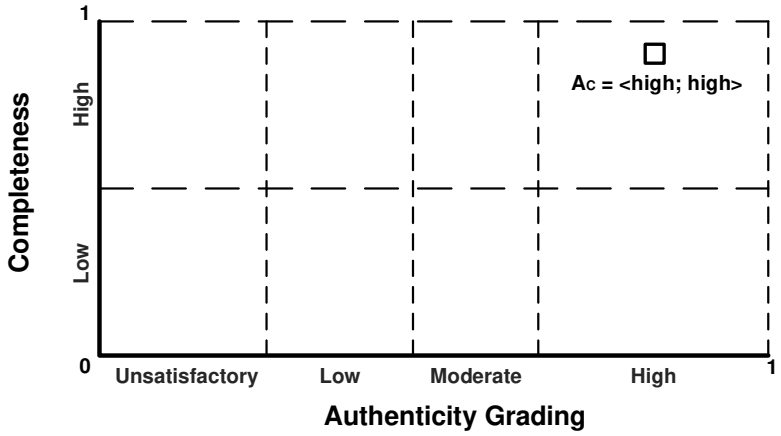

Figure 4. Authenticity classification graph.

The authenticity classification graph in Figure 4 shows a visual representation of the final authenticity classification. The x-axis represents the authenticity grading scale; the vertical lines divide the space into four quartiles corresponding to the four grades of authenticity. The y-axis represents the completeness scale; the single horizontal line distinguishes between high confidence and low confidence. The square in the top-right corner of the graph shows an example authentication classification of A_C = <high; high>.

4. Authenticity Classification Tool

A proof-of-concept tool was developed to automate the computation of the authentication classifications of smartphone data. Although a digital forensic professional could perform the computations manually, the automation eliminates human error and supports the visualizations of the results.

4.1 Tool Description

The tool computes and presents the authenticity classifications of evaluated smartphone data. Specifically, the tool supports the evaluation of all the assessment points of all the requirements. Note that each assessment point has one of three outcomes: yes (= +1), no (= –1) or absent (= 0). Equations 1 through 5 are used to compute an overall authenticity classification.

Figure 5 shows the user interface of the tool. The central viewing area has functional tabs, three interactive buttons and a canvas for rendering the authenticity classification graph. Each tab represents a com-

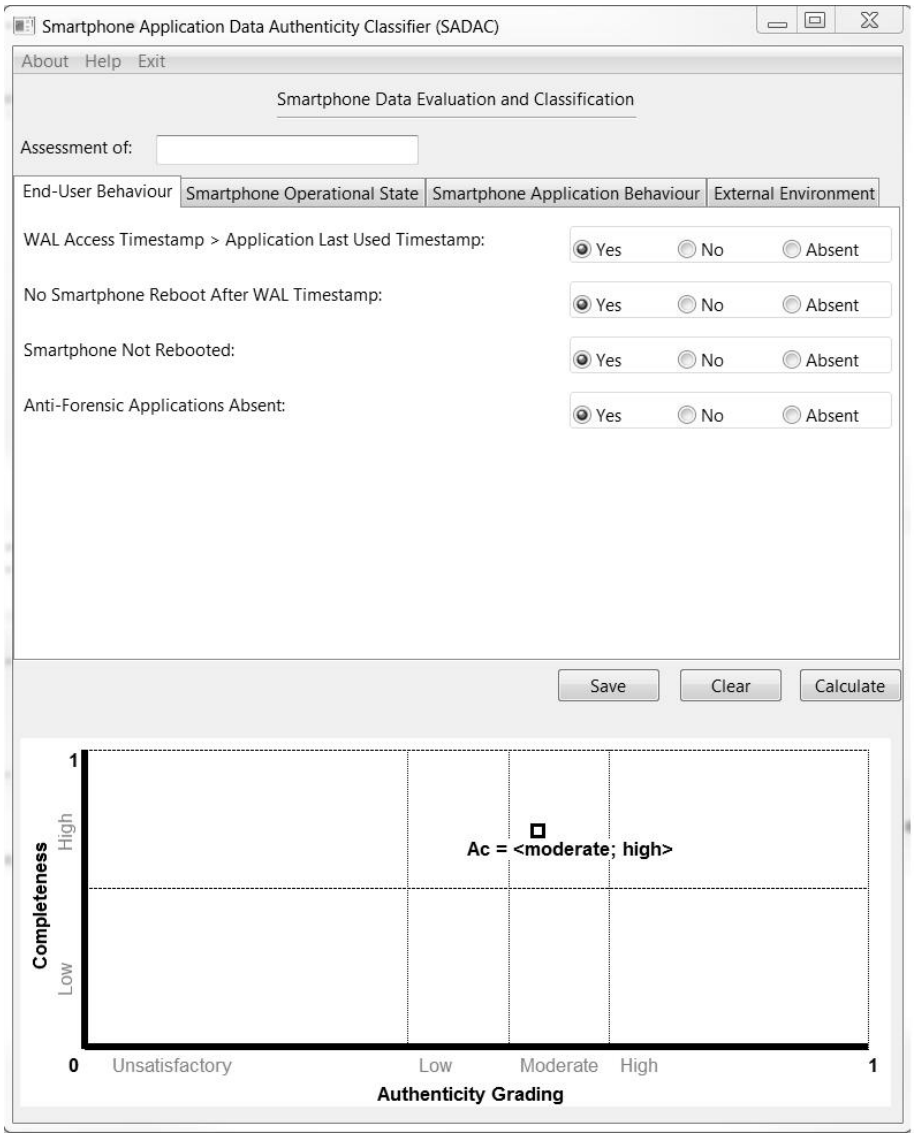

Figure 5. User interface.

ponent of authentic smartphone data and captures all the assessment points associated with the requirements for the component. Three radio buttons are provided to enter the outcomes for assessment points; the buttons ensure that only one option from yes, no and absent is selected for an assessment point. The Calculate button collects the results of all the evaluated assessment points and computes the authenticity clas-

sification. The final authenticity classification is presented within the authenticity classification graph in the canvas panel below the buttons.

4.2 Experimental Results

An experiment was conducted to validate the classification model. The experiment relied on a generic process for smartphone data manipulation [14]. The following four steps were involved in smartphone data manipulation:

- Ensure that the selected smartphone is accessible by confirming that the smartphone is either rooted (Android) or jailbroken (iOS).
- Select the application and identify the location of the files (e.g., SQLite database) that contain smartphone data.
- Identify the most appropriate approach for accessing smartphone data – either direct or off-device. The direct approach performs the manipulation of the smartphone data directly on the smartphone and relies on a program or utility to access the files. The off-device approach requires the files to be transferred to and from a connected computer with the required program or utility installed on the computer to perform the manipulation.
- Perform a manual reboot of the smartphone.

The experiment used an iPhone 7 as the test device. A new, albeit fabricated, text message was created on the device. A generic process for smartphone data manipulation was used to create the fabricated text message. The following steps were involved in creating the fabricated text message:

- Jailbreak the iPhone 7 using the `extra_recipe + yaluX` application.
- Pinpoint the storage structure (SQLite database) of the iPhone's default messaging application (`/private/var/mobile/Library/SMS/sms.db`).
- Employ the direct approach and insert a fabricated text message in the SQLite database using the pre-installed `sqlite3` command-line utility.
- Reboot the iPhone 7 to complete the manipulation process and ensure that the changes are reflected on the smartphone.

Table 3. Traces created by the experiment.

Trace	Trace Description
T_1	Automatic installation of the Cydia application
T_2	Unavailability of over-the-air updates
T_3	Discrepancies between write-ahead log file entries and application usage timestamps
T_4	Use of the `sqlite3` program
T_5	Presence of a clean write-ahead log file
T_6	Creation of entries in the reboot log file
T_7	Discrepancies in the mobile network provider records

The manipulation of the smartphone data has inherent side-effects that create various traces. Table 3 lists the traces specific to the experiment. Jailbreaking the iPhone 7 causes the automatic installation of the Cydia application and prevents over-the-air updates. Gaining access to the persistent data in the SQLite database via 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 `sqlite3` program to gain access to the persistent data, which changes the last access timestamp associated with the program. This timestamp also closely follows the last modification timestamp of the SQLite database. Accessing the SQLite database to manipulate the record causes an immediate checkpoint to occur. Therefore, after closing the SQLite database, a clean and empty write-ahead log file is present on the iPhone 7. Finally, rebooting the iPhone 7 creates a new entry in the `/var/mobile/logs/lockdownd.log` reboot log.

Note that, although this was not observed in the case of the test iPhone 7, creating a fabricated text message causes discrepancies in the records captured by mobile network providers.

The traces listed in Table 3 were used to evaluate the authenticity of the smartphone data. The outcome of the authenticity grading is expected to be low or unsatisfactory due to the changes made to the iPhone 7 when implanting the fabricated text message. A high completeness value is anticipated because all the assessment points were evaluated.

Figure 6 presents the authenticity classification of the evaluated smartphone data. The computed authenticity classification confirms the assignment of a low authenticity grading. Furthermore, the authenticity classification also confirms a high completeness value, which is antici-

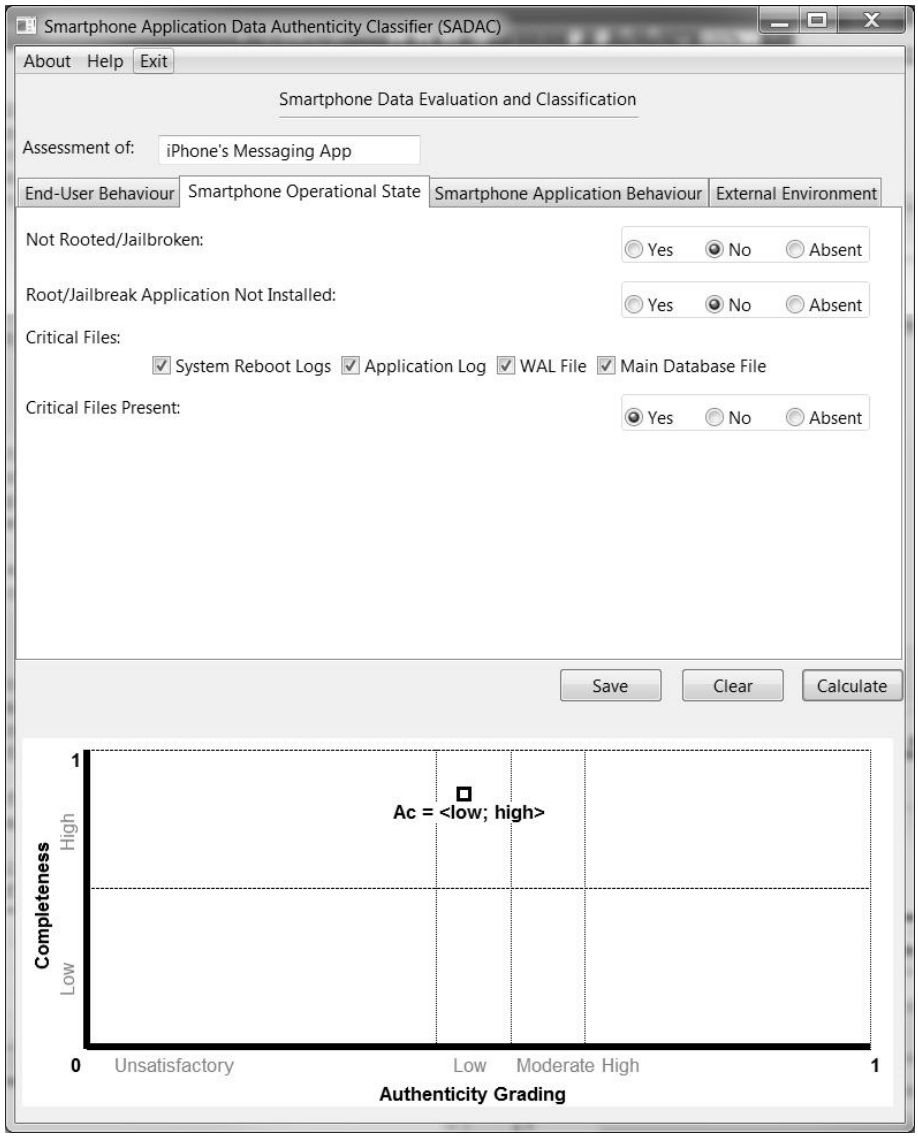

Figure 6. Experimental results.

pated because all 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 authenticity of the data.

5. Conclusions

Data extracted from smartphones provides digital forensic professionals with clear snapshots of end-user events. The value of this digital evidence mandates a formal, consistent and complete methodology for confirming its authenticity, especially since the evidence could be compromised by anti-forensics, malware or users with malicious intent. The previously-specified smartphone data evaluation model describes how to review smartphone data but does not provide a classification of data authenticity. The classification model presented in this chapter addresses this shortcoming by defining a mechanism that classifies smartphone data authenticity using a grade of authenticity and a value that conveys the completeness of the data evaluation. Experimental results confirm the effectiveness of the model in classifying the authenticity of smartphone data. The model provides significant investigatory assistance to digital forensic professionals, enabling them to pinpoint and discount or eliminate unreliable smartphone data from consideration when making investigative conclusions.

Future research will focus on handling multiple smartphone applications. Research will also attempt to identify patterns in smartphone data that could enhance or diminish the authenticity of smartphone data in digital forensic investigations.

References

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

[2] M. Bader and I. Baggili, iPhone 3GS forensics: Logical analysis using Apple iTunes Backup Utility, *Small Scale Digital Device Forensics Journal*, vol. 4(1), 2010.

[3] E. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, Academic Press, Waltham, Massachusetts, 2011.

[4] G. Cecere, N. Corrocher and R. Battaglia, Innovation and competition in the smartphone industry: Is there a dominant design? *Telecommunications Policy*, vol. 39(3-4), pp. 162–175, 2015.

[5] F. Cohen, *Digital Forensic Evidence Examination*, Fred Cohen and Associates, Livermore, California, 2009.

[6] L. Duranti, From digital diplomatics to digital records forensics, *Archivaria*, vol. 68, pp. 39–66, 2009.

[7] M. Hannon, An increasingly important requirement: Authentication of digital evidence, *Journal of the Missouri Bar*, vol. 70(6), pp. 314–323, 2014.

[8] R. Harris, Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem, *Digital Investigation*, vol. 3(S), pp. S44–S49, 2006.

[9] W. Jansen and R. Ayers, Guidelines on Cell Phone Forensics, NIST Special Publication 800-101, National Institute of Standards and Technology, Gaithersburg, Maryland, 2007.

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

[11] H. Pieterse, M. Olivier and R. van Heerden, Playing hide-and-seek: Detecting the manipulation of Android timestamps, *Proceedings of the Information Security for South Africa Conference*, 2015.

[12] H. Pieterse, M. Olivier and R. van Heerden, Evaluating the authenticity of smartphone evidence, in *Advances in Digital Forensics XIII*, G. Peterson and S. Shenoi (Eds.), Springer, Cham, Switzerland, pp. 41–61, 2017.

[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] H. Pieterse, M. Olivier and R. van Heerden, Detecting manipulated smartphone data on Android and iOS devices, in *Communications in Computer and Information Science*, H. Venter, M. Loock, M. Coetzee, M. Eloff and J. Eloff (Eds.), Springer, Cham, Switzerland, pp. 89–103, 2019.

[15] B. Schatz, Digital Evidence: Representation and Assurance, Ph.D. Thesis, Information Security Institute, Faculty of Information Technology, Queensland University of Technology, Brisbane, Australia, 2007.