The Smartphone Evidence Awareness Framework for the Users

Zama I Dlamini[1], Martin S Olivier[2], Marthie M Grobler[3]
University of Pretoria, Department of Computer Science, ICSA[1,2]
Council for Scientific and Industrial Research, DPSS, CD[1,3]
[1]idlamini@csir.co.za, [2]molivier@cs.up.ac.za, [3]mgrobler1@csir.co.za

Abstract

Smartphones are high-end mobile devices which offer more advanced computing ability and connectivity than traditional feature-phones. Not only does smartphones provide more advanced features, but it also provides mobile business to the users. This paper presents the smartphone evidence awareness (SEAware) training framework for smartphone users. This framework focuses on enhancing smartphone evidence awareness skills of smartphone users with regard to collecting, preserving and handling the related data as evidence. The proposed SEAware framework is designed to make users aware of the integrity of evidence that can be collected by an average user, resulting in the evidence being compromised by way of incorrect collection, storage or handling requirements. This framework could improve evidence preservation in cases involving smartphones as sources of evidence to confirm users' testimony during trials. It simplifies the investigation process and improves chances of admissibility of evidence at court when smartphone users are aware of the capabilities of their devices. The SEAware framework further provides instructors or trainers with sufficient guidelines on various steps they need to consider in order to deliver effective and easy to maintain SEAware training.

Keywords

Awareness, Collection, Evidence, Framework, Preservation, Safety, Smartphone

1. Introduction

According to the 2013 report by the ITU, the total mobile cellular subscriptions are expected to reach close to the landmark figure of 7 billion by the end of 2014, more than half of which are found in the developing countries (eMarketer, 2014). This increase is believed to be cultivated by the technology growth from developing countries, such as Africa, China and India, to which the mobile subscription rate is deemed to account for 78% of the world's total (mobiThinking, 2014). This is a significant growth in the use of these devices.

This paper presents the smartphone evidence awareness (SEAware) training framework for smartphone users. This framework focuses on enhancing smartphone evidence awareness skills of smartphone users with regard to collecting, preserving and handling the related data as evidence. The proposed SEAware framework is designed to make users aware of the integrity of evidence that can be collected by an average user, resulting in the evidence to it being compromised by way of incorrect collection, storage or handling requirements.

Statistics South Africa (2012) reported that mobile devices are dominantly used by the youth (60% of the South African population comprised of youth between the age of 16 and 25 years); hence, they are targeted in this study. Moreover, a study conducted by the Deloitte Digital Mobility Team early in 2014 on the use of

smartphone device Operating Systems (OSs) in South Africa found that the monthly market was different as the users buy in terms of the trends (Deloitte Digital, 2014). The Android OS (dominated by Samsung) was reported to have taken close to half of all smartphone sales and growth (Samsung, 2014). Modern phones are often equipped with a large variety of sensors, including cameras (with video recording capability), sound recorders, GPS receivers and accelerometers.

2. The Need for The SEAware Framework

Smartphones may prove to be particularly useful in case of an incident that requires evidence to be gathered. Examples include motor vehicle accidents, criminal activities and events that may become the subject of civil litigation (Stevens, 2011). However, there are certain legal requirements for such evidence to be admissible in the courtroom or used in an investigation (Blackwell, 2011; Casey, 2007). Evidence should be collected and handled in an appropriate manner. The average person on the street may be unaware of the utility of their phones to collect such evidence. The integrity of such evidence may be compromised by way of incorrect collection, storage or handling. The smartphone evidence awareness (SEAware) framework was been developed in order to set better guide for formulating the SEAware training programme to be used to make users aware of these requirements.

This is due to the developments of smartphones which change every day, making it critically significant to ensure that users understand the powerful nature of these devices as early as before owning one. This will enable mobile users to focus on getting updates on further developments of these devices. Preparing and training users on smartphone evidence will be challenging as there is no literature that focuses training users on digital evidence in general (GlobalLearning System, 2014). Currently, training of this nature targets professional responders of digital incidents than users. This is due to the reactive nature of the digital forensic subject (Grobler, 2013). Generally, the nature of training or campaigns focuses only on the user security awareness when targeting the users. Dealing with digital forensics this way lead to some challenges, such, insufficient digital evidence, digital evidence (unintentionally or unknowingly) altered with, lost or deleted files, unreported cases, etc. These could be prevented or minimised if users could be training and made aware of the role they can play on the other end. This study focuses on how users could be trained to realise and protect the integrity of raw data, so that when need be, it can be useful to the investigator or to other related parties. This could further assist in proving or disapproving the user's perspective of the case.

This paper emphasises that a successful SEAware framework is one where users are equipped with methods and skills that allow them to easily respond to incidents around them, by using their smartphone devices' capabilities, while maintaining the reliability of such captured data. The main goal of this project is to develop a Smartphone Evidence Awareness Training Programme for smartphone users.

This paper is structured as follows: the next section discusses smartphone devices and digital evidence. This is followed by the development of smartphone evidence awareness framework. The implementation aspects of the proposed framework conclude the study.

3. Smartphone Evidence and User Awareness Skills

With the advancing rate of smartphone devices, the amount and types of data that can be found in these devices is constantly increasing as well. This section focuses on different types of data (or potential evidence); the specific sources where smartphones store data, files and records, as well as the external sources, that is, sources to capture smartphone data beside the device itself. Although the user manuals that come with smartphone devices provide all the functionality of the smartphone, the user can also use the manufacturer's documentation that is normally available with this information from the sites that catalogue the capabilities of many mobile devices such as phonescoop.com or GSMarena.com (GSMA and Deloitte, 2012; Ogg, 2014).

This information guides a user in terms of the functionalities that they can use in cases of emergency, for instance, a user has been kidnapped and is on the boot of the car, using the GPS/GLONASS connection of their devices, they can determine the location as well as the directions of the car and call for help (Casey, 2011). The following subsection discusses the different types of evidence that is found on smartphone devices.

3.1. Types of Evidence on Smartphones

Due to continuous advancement of the smartphone features such as increased memory storage and third-party applications, their usage has also increased to be equally comparable to that of personal computers. These devices have also turned to be major sources of digital evidence. The quantity and complexity of evidence found on these devices increased with a similar rate (Jansen and Ayers, 2007). All these consequently pose a threat to the validity of smartphone forensics. Data that can be found on a smartphone device that may qualify as evidence includes but is not limited to pictures, call logs, SMS and MMS messaging, contact list, videos, routes, IMEI/ESN information, web browsing, Wireless network settings, geolocation information (including geotags contained within image metadata), e-mail and other forms of rich internet media, including important data such as social networking service posts and contacts which are now retained on smartphone 'apps' (Casey and Turnbull, 2011).

Table 1 tabulates the types of evidence that can found on smartphones as well as whether its smartphone generated or is network based evidence. Even though file format differs for different smartphones, they can be analysed efficiently because the file formats are common to most smartphones (Thing and Tan, 2012).

Table 1: Device- and Network-based Types of Smartphone Data (Samsung, 2014; Thing and Tan, 2012)

Types of Evidence	Device- Based	Network-Based
Call history	Yes	Yes
Contact list	Yes	No

SMS and MMS Records	Yes	Yes
Emails Records	No	Yes
Media (pictures, videos, audio) Files	Yes	No
Web Browsing History	No	Yes
Instant Messaging/ Chat Records	Sometimes	Yes
Social Network Accounts Records	No	Yes
Calendar/ Memo/ Notes Records	Yes	Sometimes
Connections (Mobile Network, Wi-Fi, and Bluetooth) Records	No	Yes
Maps (Locations, Directions Help, and Favourites) History	No	Yes
Software (Document Processing Software, VoIP Software, etc.) Used	No	Yes

3.2. Sources of Smartphone Evidence

Except for data that can be recovered from smartphones (see Table 2), sources such as base stations, towers, etc. can be used during forensic investigations. Since smartphone devices can connect to various networks via cellular towers, Wi-Fi access points, and Bluetooth, their nature creates opportunities and dangers from a forensic standpoint (Mylonas et al., 2012). Connected networks can contain useful information related to smartphone or any mobile devices. This has a potential of enabling offenders to destroy incriminating evidence remotely. Table 2 provides a breakdown of smartphone functionality in terms of sources of evidence, types of information as well as the examples of data that can be found on these sources.

Table 2: Sources of Evidence in the Smartphone

Source of Evidence	Data Type	Examples of Evidence
Smartphone	User-created information	Photographs (including EXIF data); Video/audio; maps, MMS; GPS waypoints; stored voicemail; files stored on system; connected computers
	Internet-related information	Online accounts; purchased media (often discoverable in embedded metadata); e-mail; Internet usage; social networking information
	Installed third-party applications	Alternate messaging and communication systems; additional capabilities; malware applications; penetration testing; other applications-anything can help provide alibi or tie to an individual
SIM card	Identifiers	Subscriber identifier (IMSI); SIM card identifier (ICC-

Source of Evidence	Data Type	Examples of Evidence
		ID)
	Usage information	SMS; abbreviated dial names/ numbers; last dialled numbers; location areas

Table 3 shows a summary of the smartphone- related data that can be found from other different sources other than the smartphone device itself, such as, local workstations of the smartphone owner and carriers (Casey, 2004). This type of information is classified according their type.

Table 3: Other Sources of Smartphone Evidence

Source of Evidence	Data Type	Examples of Evidence
Local Workstation	Transferred information	Tethered mobile devices; backed up phone data; backed-up third-party applications; store accounts; purchased media
Carriers	Tracking information	Connected cell towers over time; location at different times; current location (inaccurate) (Mylonas et al., 2012; Thing and Tan, 2012)
	Usage information	Billing information; call register over time; Internet/data usage; messages not delivered (after radio isolation); be warned-SIM cloning does occur and information is not to be taken at face value (Mylonas et al., 2012; Thing and Tan, 2012)

To emphasise this further, the incidents and smartphone evidence are presented against the taxonomy of evidence type (which derived from a set of questions: *who* did it – for identity evidence; *where* did it happen – for location evidence; *when* did it happen – for time evidence; *what* happened – for context evidence; *why* did it happen – for the motivation evidence; *how* did it happen – for the means evidence) (Jansen and Ayers, 2007). These questions are being used in Digital Forensics literature (Casey, 2011; Casey and Turnbull, 2011; Jansen and Ayers, 2007) for evidence examination and analysis, as well as for evidence presentation in courts of law.

For example, in Table 4 (where 'Y' stands for 'Yes', 'N' stands for 'No' and '?' stands for 'Not sure'), identity and location evidence could be found on all types of incidents and smartphone data. This is evidence that identify subjects that are part of an incident as well as approximate or exact location, where an event takes place; respectively. While navigation and network mobility records of the smartphone device might sometimes not reveal the time (time evidence) that an incident took place or the motive (motivation evidence) behind the incident; it is impossible to extract user actions and activities for an incident description or the incident nature (context evidence) and the way (means evidence) that an incident took place or the mean that were used.

Table 4: Incidents, Smartphone Evidence against Taxonomy of Evidence Type

Name of incident	Smartphone Evidence	Who	Where	When	What	Why	How
Seeking directions, looking for a route, navigation (lost, looking for direction, directing someone)	Navigation records, network mobility records	Y	Y	?	N	?	N
Murder, killing, shooting, stabbing (on self-defence, witnessing it, spotting/ finding it)	All smartphone data	Y	Y	Y	?	?	Y
Hijacking (a victim of, witness it)	Media (pictures, videos, audio) Files	Y	Y	Y	?	N	Y
Housebreaking, burglary (a victim of, witness it)	Media (pictures, videos, audio) Files	Y	Y	Y	?	N	Y
Kidnapping, held on hostage, abduction, false imprisonment (a victim of, witness it)	Media (pictures, videos, audio) Files, Call history, SMS and MMS Records, Navigation records, network mobility records	Y	Y	Y	Y	?	Y
Robbery, shoplifting, purse snatching, looting (a victim of, witness it)	Media (pictures, videos, audio) Files	Y	Y	Y	Y	N	Y
(Car/ train/ bus/ plane) accident, crash, collision (a victim of, witness it)	Media (pictures, videos, audio) Files, Navigation records	Y	Y	Y	N	N	Y
Stalking, flaming, insulting, threatened, bullying (a victim of, accused for, witness it)	All smartphone data	Y	Y	Y	Y	?	Y

3.3. Awareness Skills of Smartphone Users

In the context of smartphone forensic and investigations, processes such as preparation, planning, acquisition, analysis and presentation environment; smartphone users do not have adequate awareness skills to handle (collection and preservation) smartphone evidence with integrity that can improve that evidence's admissibility to the court of law. According to Rezgui and Marks (2008), being aware means having knowledge and being well informed about a particular event, the development of a situation or a fact. Security awareness training is used to equip

the recipients or affected audience on the security risks and countermeasures skills (GlobalLearning System, 2014). From the security awareness training, the audience develops cyber-security skills and expected security practise. Security awareness campaigns are most common within organizations and communities. This study reviewed both sources. This section lays the background on smartphone evidence and users awareness skills (Peltier, 2005). The formulation of the smartphone evidence awareness framework is discussed in the next section.

4. Development of Smartphone Evidence Awareness Framework

In order to participate in the SEAware training, the trainee needs to have fundamental understanding of the basic use of a smartphone device and installation of mobile applications. The SEAware training framework therefore consists of five main components, namely:

- Basic smartphone background,
- Role of evidence,
- Smartphone evidence collection,
- Smartphone evidence preservation, and
- User safety measures.

These factors were formulated following the guidelines for formulating a training curriculum from the South African Qualification Authority (SAQA) (South African Qualifications Authority (SAQA), 2001).

4.1. Basic Smartphone Background Information

This learning component lays a significant background about smartphone devices, including:

- differences amongst various types of smartphones,
- current uses of smartphones,
- future trends of smartphones, and
- advantages and disadvantages of using smartphones.

The smartphone background learning component (in Figure 1) covers various topics, including definition of smartphones, smartphone usage statistics, a comparison between smartphones and feature phones, smartphones and their operating systems, capability and capacity of smartphones as well as smartphone multimedia..

Figure 1: Smartphone Background Learning Component

Other topics that can be included could be trends of smartphone devices as well as advantages and disadvantages of using smartphones. The outcome of this learning component includes trainees' ability to identify smartphone uses, capabilities, advantages and disadvantages and future trends. It provides smartphone users with basic uses of smartphone devices, such as calling, texting, apps installation, searching locations using GPS, capturing pictures, videos, audio, etc. When the background details about smartphone devices have been presented, it is imperative to also look at the role of evidence found on smartphones. This is the second learning component of the SEAware training framework, and is discussed in the next subsection.

4.2. Role of Evidence

The role of the evidence learning component is to present details on the role of evidence in general and more specifically about smartphones. In order to achieve this goal, this outline must be followed:

- Define evidence in general,
- Emphasise different types of evidence,
- Describe rules regarding evidence, and

This component (in Figure 2) presents the definition of the smartphone evidence as all traces of smartphone related data presented to a court as a proof of the facts to the issue and which may include the testimony of witnesses, records, documents, or objects. This is in effort to fulfil the general rules of evidence such as relevance, authenticity, reliability as well as chain of custody (Casey, 2011; Grobler et al., 2011; Grobler and Dlamini, 2012; Rogers et al., 2006).

Figure 2: Role of Evidence

These topics, in Figure 2, are defined in such a way that they improve smartphone evidence admissibility. The outcome of this learning component includes trainees' ability to understand:

- what general and smartphone evidence is,

- differentiate between types of evidence.
- the legal aspects pertaining to smartphones,
- rules of evidence for it to be either admissible or inadmissible, and
- evidence that can prove/ disprove a claim.

The role of the evidence learning component provides smartphone users with sufficient details on the role of evidence for any investigations. When the user understands their device capabilities and have a clue about what could be regarded as evidence (as well as rules regarding how evidence have to be handled for admissibility purposes) in a court of law; understanding how smartphone evidence can be collected with integrity is also significant. This is discussed in the next subsection.

4.3. Smartphone Evidence Collection

This is the third learning component of the SEAware framework. The smartphone evidence collection learning component, in Figure 3, encourages safe collection of smartphone data. It covers smartphone functionalities, as well as data that can be found from all smartphone functionality. This includes different types of smartphone capabilities which can be used to / could automatically collect data; such as address book, planner, messenger, photo and video camera, GPS navigator, web and IM client, platform of third Part Apps (BusinessTech, 2014).

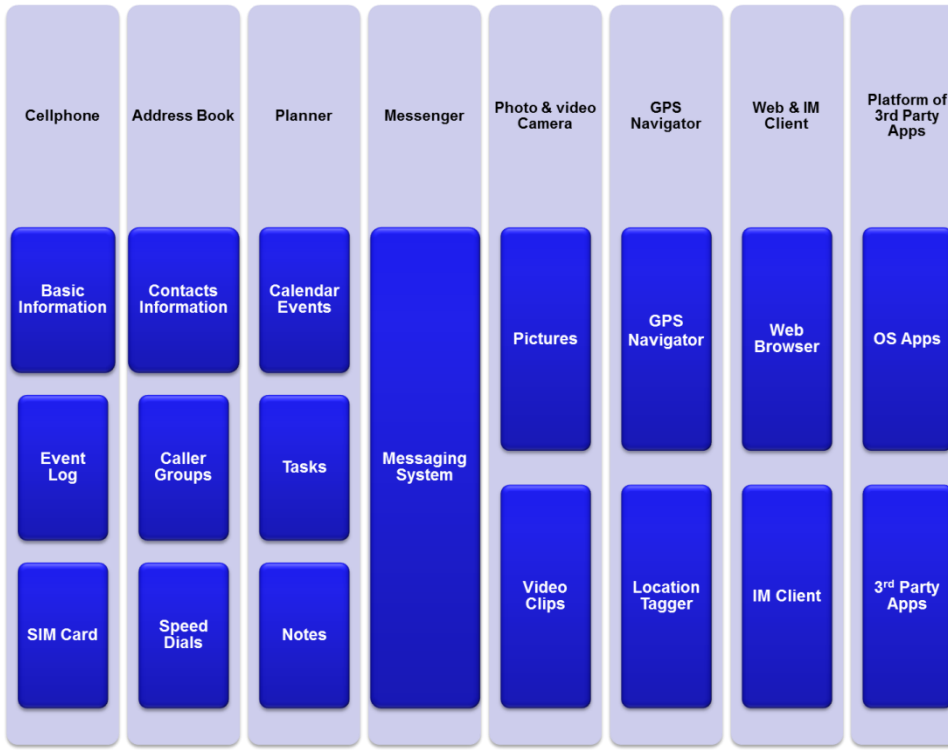

Figure 3: Smartphone Forensic Features

The smartphone data collection learning component emphasises the opportunities that can be used by the smartphone user to collect evidence, such as: taking a picture, recording a sound, capturing a video, sending/ receiving a message or text, making/ receiving a call, determining user location and making use of mobile applications. These topics enable the smartphone user to understand:

- the essence of smartphone functionalities,
- the different types of smartphone data,
- the practical problems that may be encountered when dealing with smartphone data, and
- different categories of devices that may be encountered during a smartphone investigation.

The outcome of this learning component includes trainee's ability to:

- recognise role and relevance that smartphone data can play in specific scenarios,
- distinguish types of data collected by networks without direct user interaction,
- respond appropriately to the opportunities where smartphone data can be collected usefully, and
- become aware of the data that can be collected by the network.

This learning component further provides smartphone users with smartphone data collection techniques, which will assist them in making-up their minds on best smartphone feature to use during a specific incident. These will also assist the users in identifying opportunities of safely gathering smartphone data. When smartphone evidence has been collected, it has to be handled in an appropriate manner until it is presented in court. Ways in which the smartphone user can preserve smartphone data as discussed on the next subsection.

4.4. Smartphone Evidence Preservation

The smartphone data preservation learning component identifies and discusses threats that are related to preservation of smartphone data, such as: data modification, device theft, loss, confiscation or demanded by perpetrator, storage space and period and data deletion (Casey, 2011). Smartphone evidence preservation methods assist in validating the claims made about the incident and reconstruction of events (Casey, 2007). It also focuses on methods, (as shown in Figure 4), that the smartphone user can use in order to preserve their data in a forensically sound manner. Examples of the methods one could utilise to preserve smartphone evidence include the following:

- Sending smartphone data to someone via messaging or texting.
- Printing and putting a copy of smartphone data in a sealed envelope with a date across the flipping-part of an envelope.

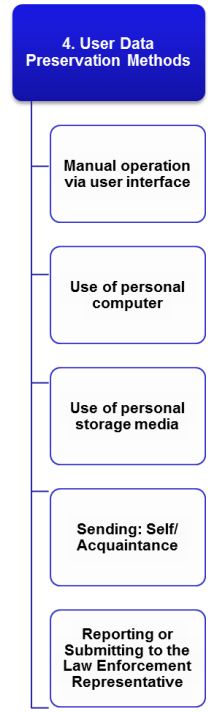

Figure 4: Smartphone Evidence Preservation Skills

- Uploading smartphone data to the cloud.
- Burning smartphone data to a CD or copying to a SD card.

The outcome of this learning component includes trainee's ability to:

- become familiar with the smartphone user data preservation methods and techniques,
- become aware of the basic principles of chain of custody regarding smartphone data, and
- learn about what to do with smartphone data that have been captured.

Since data preservation assists in validating the claims made about the incident and reconstruction of events, this learning component furnish smartphone users with skills to preserve smartphone data that have the potential to be regarded as evidence in a court of law. Enabling the smartphone user to understand the processes involved in smartphone investigation, as well as the understanding user self-preservation methods of smartphone data. In order to ensure that smartphone users stay alert and do not put their lives in danger during the collection and preservation of smartphone evidence, the learning component of user safety measures is presented on the next subsection.

4.5. Providing User Safety Measures

The user safety learning component aims at providing safety settings that smartphone user can apply on their devices in order to be prepared for most of the possible circumstance that will require their prompt response without becoming first responders. Some of the significant areas that are covered include by this learning component include:

- Smartphone personal readiness plan.
- Personal risks associated with evidence collection and preservation.
- Best practises.

This specification, illustrated in Figure 5, provides the smartphone users with safety tips regarding collection and preservation of smartphone data.

Figure 5: Safety Measure

The outcome of this learning component includes trainee's ability to:

- learn about risks associated with the collection of data in specific situations,
- be able to formulate their smartphone personal readiness plan, and
- become used to smartphone safety best practises.

This will enable the smartphone user with better response techniques to incidents while practising safety precautions. It also provides safety tips regarding collection and preservation of smartphone data.

5. The SEAware Training Framework

The SEAware training components were incorporated, as shown in Figure 6, to form the SEAware training framework. This framework consists of a set of basic concepts which determine the savviness of smartphone users, enhance the safe smartphone evidence collection and preservation and improve smartphone evidence admissibility at court. The SEAware training should start with laying the background of smartphone devices, shown as number one in Figure 6. This is followed by the details on legal issues, as far as smartphone evidence is concerned in number two of the components. Component number three includes smartphone data collection per smartphone capability. The fourth component covers user data preservation methods. Lastly, safety measures component equips smartphone user with better response techniques to incidents while practising safety precautions.

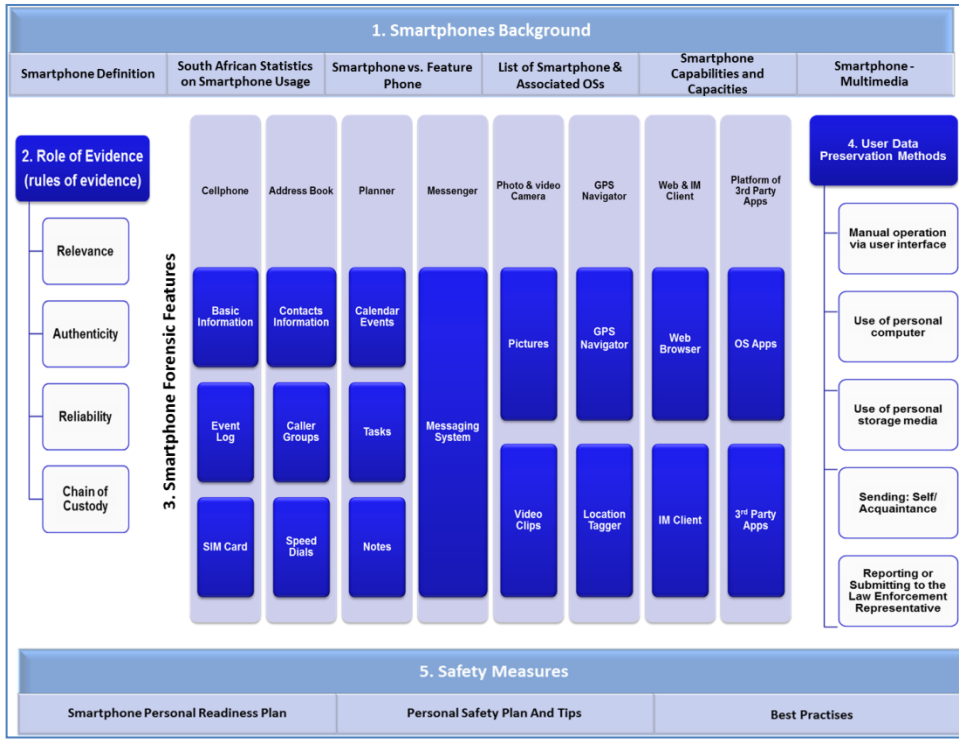

Figure 6: SEAware Training Framework

In the context of smartphone forensic and investigations processes such as preparation, planning, acquisition, analysis and presentation environment presented in section 3, the learning components identified in section 4 becomes desirable in order to achieve an effective SEAware training for smartphone users. The SEAware implementation plan, in Table 5, illustrates general components of security awareness and their description in the context of SEAware training which could be followed for the process of formulating SEAware training material (Peltier, 2005). Using the general awareness components on the first column of Table 5, the SEAware training programme is described on the second column.

Table 5: SEAware Implementation Plan

Awareness Component	Description
Goal / Purpose	The main purpose of the training is to make smartphone users aware that their devices could be good sources of digital evidence, which might be inadmissible in a court of law if it is not handled properly
Objective	- To test smartphone evidence awareness skills before and after the training

Awareness Component	Description
	- To train a group of smartphone users on effective ways of safely collecting and preserving admissible data - To present analysed results and recommendation
Awareness Need	- Nature of digital evidence tends to lead to the inadmissibility of such evidence in court - High influx of smartphone devices and their applications - From the smartphone users' point of view, evidence can be recovered from their handset memory and in- and/or out-boxes. To the average smartphone user, deleting such data from these locations means that it is gone forever; it is a different story to digital investigators.
Campaign Name	Smartphone Evidence Awareness
Stakeholder	Smartphone User
Topics Cover	- Smartphone background (see section 4.1) - Role of evidence (see section 4.2) - Smartphone evidence collection (see section 4.3) - Smartphone evidence preservation (see section 4.4) - User safety measures (see section 4.5)
Target Audience	Smartphone users
Delivery Methods	Presentation and group discussion
Evaluation	Pre- and Post- Questionnaire

6. Benefits of the SEAware Framework

The SEAware framework has been developed to make users aware of the integrity of evidence that can be deliberately collected by an average user, resulting in it being compromised by way of incorrect collection, storage or handling requirements. The effect of this programme is evaluated through the development and experimental implementation of the SEAware training material (in Table 5) to a group of smartphone users). This paper presented the major aspects of the SEAware training framework that could benefit the user as follows:

- Smartphone capabilities: provides smartphone user with basic uses of smartphone devices, such as calling, texting, apps installation, searching locations using GPS, capturing pictures, videos, audio, etc.

- Role of digital evidence: provides smartphone user with sufficient background on role of evidence in any investigations.
- Collection of smartphone data: provides smartphone users with smartphone data collection techniques, which will assist the smartphone users in making their mind on best smartphone feature to use during a specific incident.
- Preservation of smartphone data: furnishes smartphone users with skills of preserving smartphone data that have potential to be regarded as evidence at court of law.
- User safety measures: provides safety tips regarding collection and preservation of smartphone data.

This proposed framework could improve evidence preservation in cases where smartphones devices are used as source of evidence to confirm users' testimony during trials. Despite the purpose of recording or capturing; smartphones can compile a complete list of all applications with data that can prove that the user have or have not committed crime, that is, using a it as an alibi, or using it as an evidence collection tool. This simplifies the investigation process and improves admissibility of evidence at court when smartphone users are aware of the capabilities of their devices.

7. Conclusion and Future Work

Many people carry devices with them that may be valuable in evidence gathering and preservation. Modern phones are often equipped with a large variety of sensors, including cameras (with video recording capability), sound recorders, GPS receivers and accelerometers. The integrity of such evidence may be compromised by way of incorrect collection, storage or handling. This paper proposes a smartphone evidence awareness (SEAware) training framework to be used make users aware of these requirements. This framework could improve the current level of skills to properly collect and preserve admissible smartphone evidence at user level.

Future work includes the development of the SEAware training programme, which will consist of training material and evaluation measures, such as questionnaire. The SEAware training programme will further be tested on different groups of smartphone users to test its viability.

8. References

Blackwell, C., 2011. An Investigative Framework for Incident Analysis VII, 23–34.

BusinessTech, 2014. South Africa's most popular smartphone brands [WWW Document]. URL http://businesstech.co.za/news/mobile/65048/south-africas-most-popular-smartphone-brands/ (accessed 9.27.14).

Casey, E., 2011. Digital evidence and computer crime: Forensic science, computers, and the internet. Access Online via Elsevier.

Casey, E., 2007. What does "forensically sound" really mean? Digit. Investig. 4, 49–50.

Casey, E., 2004. Network traffic as a source of evidence: tool strengths, weaknesses, and future needs. Digit. Investig. 1, 28–43.

Casey, E., Turnbull, B., 2011. Digital evidence on mobile devices, in: Digital Evidence and Computer Crime. Elsevier Inc., Baltimore, MD, USA, pp. 1–44.

Deloitte Digital, 2014. Android vs BlackBerry vs iSO vs Symbian vs Windows Phone in South Africa [WWW Document]. URL http://deloittedigital.co.za/assets/pdf/mobile-operating-systems-south-africa.pdf (accessed 9.27.14).

eMarketer, 2014. Smartphone Users Worldwide Will Total 1.75 Billion in 2014 [WWW Document]. URL http://www.emarketer.com/Article/Smartphone-Users-Worldwide-Will-Total-175-Billion-2014/1010536 (accessed 2.2.14).

GlobalLearning System, 2014. Security Awareness Training [WWW Document]. URL http://www.globallearningsystems.com/products/individual/security-awareness-training/

Grobler, M., 2013. The Need for Digital Evidence Standardisation. Emerg. Digit. Forensics Appl. Crime Detect. Prev. Secur. 234.

Grobler, M., Dlamini, Z., 2012. Global cyber trends a South African reality. [WWW Document]. URL https://ujdigispace.uj.ac.za/handle/10210/10454

Grobler, M., Dlamini, Z., Ngobeni, S., Labuschagne, A., 2011. Towards a cyber security aware rural community, in: Proceedings of the 2011 Information Security for South Africa (ISSA) Conference. Presented at the Information Security for South Africa (ISSA), Hayatt Regency Hotel, Rosebank, Johannesburg, South Africa, p. 7.

GSMA, Deloitte, 2012. Sub-Saharan Africa Mobile Observatory 2012 [WWW Document]. URL http://www.gsma.com/publicpolicy/wp-content/uploads/2013/01/gsma_ssamo_full_web_11_12-1.pdf (accessed 11.20.14).

Jansen, W., Ayers, R., 2007. Guidelines on cell phone forensics. NIST Spec. Publ. 800, 101.

mobiThinking, 2014. Global mobile statistics 2014 Part A: Mobile subscribers; handset market share; mobile operators [WWW Document]. URL http://mobithinking.mobi/mobile-marketing-tools/latest-mobile-stats/a?dm_switcher=true (accessed 9.29.14).

Mylonas, A., Meletiadis, V., Tsoumas, B., Mitrou, L., Gritzalis, D., 2012. Smartphone Forensics: A Proactive Investigation Scheme for Evidence Acquisition, in: Information Security and Privacy Research. Springer, pp. 249–260.

Ogg, E., 2014. Smartphones killing point-and-shoots, now take almost 1/3 of photos — Tech News and Analysis [WWW Document]. URL https://gigaom.com/2011/12/22/smartphones-killing-point-and-shoots-now-take-almost-13-of-photos/ (accessed 10.21.14).

Peltier, T.R., 2005. Implementing an Information Security Awareness Program. Inf. Syst. Secur. 14, 37–49.

Rogers, M.K., Goldman, J., Mislan, R., Wedge, T., Debrota, S., 2006. Computer forensics field triage process model. Presented at the Conference on digital forensics, security and law.

Samsung, 2014. Samsung GALAXY S5 [WWW Document]. URL http://www.samsung.com/global/microsite/galaxys5/specs.html (accessed 10.27.14).

South African Qualifications Authority (SAQA), 2001. Criteria and Guidelines for Assessment of NQF Registered Unit Standards and Qualifications, 1st ed. South African Qualifications Authority, Brooklyn, South Africa.

Stevens, D.J., 2011. Media and criminal justice: The CSI effect, 1st ed. Jones & Bartlett Publishers, Boston, USA.

Thing, V.L., Tan, D.J., 2012. Symbian smartphone forensics and security: recovery of privacy-protected deleted data, in: Information and Communications Security. Springer, pp. 240–251.