https://doi.org/10.48009/2_iis_2016_170-182

THE DESIGN OF SMARTPHONE EVIDENCE AWARENESS (SEAWARE) TRAINING

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

ABSTRACT

This study focuses on the Smartphone Evidence Awareness skills of smartphone users with regard to collecting, preserving and handling such data. This paper presents the smartphone evidence awareness training program. This training program is consists of the SEAware curriculum that outlines the topics that were included in the SEAware training. This curriculum was converted into a PowerPoint presentation to form part of the SEAware training material. Coupled with the training material, was a SEAware questionnaire. The SEAware training program equips smartphone users with safe methods of collection relevant smartphone data for the specific circumstances.

Keywords: Smartphone, Evidence, Awareness, Training, Safety, Collection, Preservation, SEAware

INTRODUCTION

The number of smartphone devices and smartphone users is estimated to be more than one billion worldwide *(Nielsenwire, 2012; PC Magazine, 2011).* This means that now more than ever, the majority of people are walking around with valuable information in their hands. Smartphones store various types of information, including personal identifiable information such as identity credentials, email, SMS and MMS messages, GPS coordinates, passwords and company documents *(eMarketer, 2014)*. Moreover, smartphones offer connectivity to access information from organizational servers, allowing individuals to do work anywhere. It therefore comes as no surprise that Eric Schmidt – Google CEO has the following to say about these mobile devices:

"…Smartphones are more powerful than supercomputers were a few years ago, and we are putting them in the hands of people who've never had anything like it before." - Google CEO Eric Schmidt *(PC Magazine, 2011)*. In developed countries smartphones have become a necessity because they are the most affordable and advanced computing devices. Hence, smartphone manufacturing companies have developed much cheaper devices to attract users globally. With a remarkable growth in popularity and their involvement in most aspects of our daily life; smartphones have turned into enormous evidence storage devices. Many people carry devices with them that may be valuable in evidence gathering. Modern phones are often equipped with a large variety of sensors, including cameras (with video recording capability), sound recorders, GPS receivers and accelerometers. 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 *(Duncan, 2014; Mamello, 2014).* However, there are certain legal requirements for such evidence to be admissible in the courtroom or used in an investigation. Evidence should be collected and handled in an appropriate manner without any contamination or modification of any kind.

Smartphone devices, apart from basic cellphone capabilities for calling and texting, offer advanced computing ability and connectivity. Some of these devices' features include, but are not limited to voice calling, video calling, digital camera, media player, Global Positioning System (GPS) navigation and many more. The results of these devices' ease of use, accessibility and prevalence in every aspect of our daily lives are immeasurable. Smartphone data can be used in almost any crime. The lack of user awareness as far as preservation smartphone data as well as their knowledge on the forensic features of their devices is very limited. This is confirmed in numerous occasions where evidence on smartphones is not considered significant due to the lack of awareness from both the police officials and the device users. This was witnessed on the case of Molemo "Jub Jub" Maarohanye and Themba Tshabalala, where police officials allowed the suspects to delete some of the files from their devices before seizing them *(Vuyo Mkize of IOL News, 2012).* Currently, there is sufficient information on how users can secure their information on their smartphones and very limited information on how smartphone users can knowingly or unknowingly temper with digital evidence on smartphones. The

SEAware program which is the smartphone evidence awareness creates smartphone evidence awareness on digital data contained on smartphone devices that can potentially be used as evidence at court. From smartphone users' point of view, evidence can only be recovered from their devices' memory and in- and outboxes. Deleting such data from these locations to them means it is gone forever, while it is something else to the digital investigators. The main purpose of this study 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. This paper presents the design of the smartphone evidence awareness (SEAware) training program for smartphone users. This training program presents preservation methods and good practises to the smartphone users for their handset devices when evidence is contained; and proper procedures to follow in response to such incidents where their devices are involved. The main goal of this project is to develop and test a Smartphone Evidence Awareness Training Program for smartphone users. This is a long term project made up of three phases, as illustrated in Figure 1 of the SEAware research plan. This paper focuses on the second phase of the project. The goal of this phase is to use the SEAware framework resulted on the first phase and research design methods to design a SEAware training program that can be used to train smartphone users on significance of smartphone evidence and how they can handle it with integrity to maintain its authenticity.

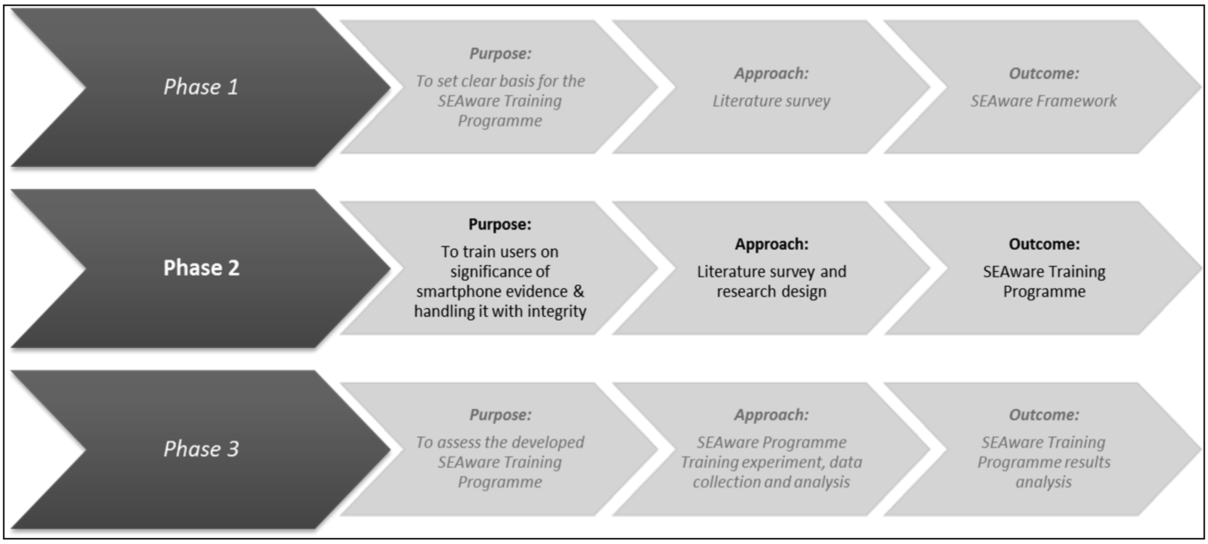
Phase 1
Purpose:
To set clear basis for the SEAware Training Programme
Approach:
Literature survey
Outcome:
SEAware Framework
Phase 2
Purpose:
To train users on significance of smartphone evidence & handling it with integrity
Approach:
Literature survey and research design
Outcome:
SEAware Training Programme
Phase 3
Purpose:
To assess the developed SEAware Training Programme
Approach:
SEAware Programme Training experiment, data collection and analysis
Outcome:
SEAware Training Programme results analysis

Figure 1. Smartphone Evidence Awareness (SEAware) Research Plan

This work improves evidence preservation in cases where smartphones devices are used as source of evidence to boost users' cases. This is especially on the use of their smartphone capabilities. Despite the purpose of recording or capturing, it can compile a complete list of all applications with data that can prove that the user have or not committed crime, that is, using a smartphone as an alibi, or using it as an evidence collection tool. 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 training program 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. The rest of the paper is structured as follows: the next section discusses the background of the study which is consists of the overview of the SEAware training framework, user skills, awareness process and South African Qualifications Authority (SAQA) assessment process. This is followed by the section presenting the design of the SEAware training program for smartphone users, which is consists of the curriculum, the questionnaire and the training presentation. This is followed by the section that shows how the SEAware training program was applied to conform to the general awareness process. This is followed by the section that presents the benefits of the SEAware training program as well as the conclusion section.

BACKGROUND

The SEAware training program is in a form of presentation slides. It is designed specifically to train smartphone users on the significance of safe collection of smartphone data and how to preserve it in such a way that it can be used as evidence in legal proceedings if need be. The training covers smartphone background information, the user collection and preservation methods of smartphone data, as well as user safety measure. This training focuses on smartphone evidence and does not cover other Digital Forensic investigation activities such as seizure, examination and analysis. The aim of the training is to educate ordinary smartphone users, familiar with mobile app installation in the correct chain of custody of digital evidence when using smartphones. This will allow the digital evidence, whether it is an SMS, WhatsApp message, photo or missed call, to be used in a legal or civil case, or submitted to court if need be. Table 1 presents the learning categories, components and description.

Smartphone Devices and Digital Evidence

A smartphone is a type of mobile phone that have widely proliferated the mobile device market more than any type world-wide *(eMarketer, 2014)*. It is defined as a high-end mobile phone that offers more advanced computing ability and connectivity than a feature or a contemporary phone *(BusinessTech, 2014)*. Smartphones run complete OS software that offers a standardized interface and platform for application developers. These devices combine both mobile phone and handheld computer features into a single device, but with additional functionality from the Mobile Computing platform. They provide advanced connectivity and computing ability as compared to the featured cellphones *(Hosmer et al., 2011)*. Smartphones provide for information storage, program installations, as well as the use of a mobile phone in one device. Smartphones can be viewed as the successors of the PDA devices. Smartphones share numerous features and applications with PDAs in form and functionality, that is, a smartphone combination of both phone and PDA *(PC Magazine, 2011)*. Smartphones usually use these mobile OS: Apple's iOS, Google's Android, Microsoft's Windows Phone, Nokia's Symbian, and RIM's BlackBerry OS *(Hosmer et al., 2011)*. Smartphones combine calendars, games, personal navigation, media players, Internet access, and cameras *(PC Magazine, 2011)*. Depending on the manufacturer or the brand, there are many other applications that come inherently with the device’s operating system, while other applications can be downloaded. In addition, email systems from mobile devices can be seamlessly synchronized with the email system accessed from computers, private or work-related emails. Some of the examples of Smartphones include, Sony Ericsson, Palm Treo, Blackberry, Nokia T-Mobile Sidekick, Torq, Motorola Q, E-Ten, HP iPaq, i-mate, and many more. Smartphones will form the foundation of this study. With the total number of smartphones users estimated to be about 1.76 billion by eMarketer (2014), this is more than 25% over 2013.

Smartphone Users and Digital Evidence

Casey (2007) believes that Digital Forensic process includes investigation of digital communication devices and storage to approve or disapprove suspicious illegal activities of the device *(Casey, 2007)*. A major misconception about Digital Forensics is the cinema and popular TV series like Crime Scene Investigator (CSI) and Naval Criminal Investigative Service (NCIS) *(Ferguson, 2013; Mukasey et al., 2008)*. Although, the technology portrayed is more or less correct, the processes and the amount of personnel and time requirements are grossly under exaggerated *(Association of Chief Police Officers (ACPO), 2008)*. These popular programs lead to the two sides of the "CSI Effect". On one hand, the criminals think they know how to commit a crime and not get caught *(Ferguson, 2013; Stevens, 2011)*. On the other hand, the average user has exaggerated expectations from technology and law enforcement agencies. It is therefore significant for legal representatives and society to realise what forensics can and cannot do *(Brodie, 2008 &* Arthur, Olivier & Venter, H., 2007 *)*. This study focuses only on the Digital Forensics awareness of smartphone devices, as these devices are commonly used and regarded as the device of preference when it comes to accessing Internet *(Ogg, 2014)*. While it makes sufficient sense to train in and maintain the skills and understanding in Digital Forensics to the Digital Forensic practitioners; it will also be more useful to consider including the other groups that are equally affected by this topic, that is, the law enforcement professionals, industry and government professionals, as well as the general public or society. This way affected parties contributes towards better investigation process with sufficient and admissible digital evidence. This study focuses on the users as this group is often left out when it comes to digital evidence trainings.

The Overview of the SEAware Training Framework

In order to participate on 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 is therefore consists of five main components, namely:

- Basic smartphone background,

- Role of evidence,
- Smartphone evidence collection,
- Smartphone evidence preservation, and
- User safety measures

These components were formulated following the guidelines for formulating a training curriculum and its assessment process from the South African Qualification Authority (SAQA) *(South African Qualification Authority, 2001) (SurveyMonkey, 2008)*. This document (by SAQA *(South African Qualification Authority, 2001)*), provides guidelines for the assessment policies, systems and procedures of SAQA accredited Education and Training Quality Assurance bodies (ETQA's) and their constituent providers. Broadly, the guidelines cover the following areas:

- Good assessment practice as it relates to the National Qualification Framework (NQF),
- The role of registered assessors,
- The assessment process, and
- Moderation of assessment

The SEAware training components were incorporated together to form a SEAware training framework. This framework is 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. This is followed by the details on legal issues, as far as smartphone evidence is concerned. The third component includes smartphone data collection process 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 practicing safety precautions. In the context of smartphone forensic and investigations processes such as preparation, planning, acquisition, analysis and presentation environment, these learning components are desirable in order to achieve an effective SEAware training framework for smartphone users. These components were explored into details when formulating the curriculum, the questionnaire as well as the training material (all presented in the next section).

DEVELOPMENT OF SEAWARE TRAINING PROGRAM

The SEAware training program is consists of the SEAware curriculum, the questionnaire as well as the training material. These are presented in this section.

SEAware Curriculum Development

The SEAware curriculum was formulated from the reviewed literature on smartphone devices, Digital Forensics, smartphone evidence and awareness. Further guidelines for formulating a training curriculum and effective assessments from South African Qualification Authority (SAQA) were followed *(South African Qualification Authority, 2001)*.The main aim of the SEAware program is to educate smartphone users, who are familiar with mobile apps installation, on the correct chain of custody of digital evidence when using smartphones. It is developed specifically to train smartphone users on the significance of safe collection of data and how to preserve it in such a way that it can be used as evidence in legal proceedings when the need arise. The SEAware curriculum consists of five training components, that is; smartphone background information, the role of evidence in general, the user collection and preservation methods of smartphone data, as well as user safety measure. These components are divided into two, which is, generic and specialization learning components. SEAware curriculum (in Table 1) has a basic smartphone background as a learning component. This is a generic learning component the rest are all specialization learning components. These are described further below.

a) Basic Smartphone Background: This is a generic core learning component that formally lays a significant background of smartphone devices. It focuses on describing differences amongst various types of smartphones, current uses of smartphones, future trends of smartphones as well as advantages and disadvantages of using smartphones. This learning component provides smartphone user with basic uses of smartphone devices, such as calling, texting, apps installation, searching locations using GPS, capturing pictures, videos, audio. This learning component provides smartphone user with sufficient background on smartphone basic background, including user's ability to: identify smartphone uses, capabilities, advantages and disadvantages and future trends.

b) Role of Evidence: This is one of the specialization core learning components that is aimed at presenting the background role of evidence in general. This was achieved by defining evidence in general; emphasizing different types of evidence and by describe rules regarding evidence. This learning component provides smartphone user with sufficient background on role of evidence in any investigations, including user's ability to learn about the make-up of evidence, differentiate between types of evidence and be aware of rules of evidence to increase its admissibility chances, identify evidence that can prove or disprove a claim.

c) Smartphone Evidence Collection: The smartphone data collection specialization core learning component aims at preparing smartphone users with safe methods of collecting relevant smartphone data for specific circumstances which users can find themselves in. The smartphone data collection specialization core learning component emphasizes the opportunities that can be used by the smartphone user to collect evidence, such as, defining types of smartphone data regarding data collection; outlining other means of smartphone data collection that do not require user's partaking; emphasizing opportunities that can be used by the smartphone user to collect evidence relevant to specific circumstances they may find themselves in. These will help smartphone users with decisions on the best smartphone feature to use during a specific incident.

d) Smartphone Evidence Preservation: The smartphone evidence preservation specialization core learning component, aims at equipping smartphone users with appropriate skills of preserving smartphone data while maintaining evidence's chain of custody. This specialization core learning component identifies 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. It also focuses at methods that the smartphone user can use in order to preserve their data in a forensically sound manner, such as sending smartphone data to someone via messaging or texting; putting a copy of smartphone data in a sealed envelope with a date across the flipping-part of the envelop; uploading smartphone data to the cloud and/ or burning smartphone data to the CD or SD card. Smartphone data preservation learning component assists users in validating the claims made about the incident and reconstruction of events.

e) User Safety Measure: The user safety measure specification core aims to provide safety settings that smartphone users can apply on their devices in order to be prepared for most of the possible incidents which will require their prompt response whilst not becoming first responders. This specification provides the smartphone users with safety tips regarding collection and preservation of smartphone data. It further provides users with smartphone personal readiness plan, personal safety plan and best practices. This provides the smartphone user with better response techniques to incidents while practicing safety precautions.

Table 1. Learning Component and their Descriptions

	UNIT 1: Smartphone Background	**UNIT 2: Smartphone Data Collection**	**UNIT 3: Smartphone Data Preservation**	**UNIT 4: User Safety Measures**
Purpose	To lay a background of smartphone devices	To equip smartphone users with safe methods of collecting relevant smartphone data for specific circumstances	To equip smartphone users with appropriate skills of preserving smartphone data while maintaining evidence chain of custody	To equip smartphone users with safety techniques they can use to use before (on their devices to be always prepared), during (collection) and after (preservation) incidents without becoming first responders
Learning/ Training Assumed in Place	Smartphone ownership, basic use and apps installation experience	-Basic smartphone background	-Basic understanding of smartphone data collection techniques	-Basic understanding of smartphone data preservation skills
Specific Outcome	Knowledge, skills, attitude and content/ underpinning knowledge			
Moderation	It applies to the whole SEAware Training Topic			

	UNIT 1: Smartphone Background	UNIT 2: Smartphone Data Collection	UNIT 3: Smartphone Data Preservation	UNIT 4: User Safety Measures
Embedded Underpinning Knowledge	Understanding smartphone uses, capabilities, advantages and disadvantages and future trends	- Understanding different types of smartphone data and their collection methods - Recognising role and relevance that smartphone data can play in specific scenarios - Understanding risk associated with the collection of data in specific situations - Understanding types of data collected by networks without user effort	- Understanding the smartphone user data preservation methods and techniques - Understanding the basic principles of chain of custody regarding smartphone data - Understanding what to do with smartphone data that have been captured - Understand duration of data preserved by the Network	- Understanding easy tips and apps to use in preparation to gather and preserve smartphone data - Understanding user safety best practises
Critical Outcomes	Basic uses of smartphone devices, such as calling, texting, apps installation, searching locations using GPS, capturing pictures, videos, audio, etc.	Able to identify the safe opportunity to safely gather smartphone data	Have skills of preserving smartphone data that have potential to be regarded as evidence at court of law	Can identify risks associated with gathering and preserving user smartphone data

This SEAware curriculum focuses on smartphone evidence and does not cover other Digital Forensic investigation activities such as seizure, examination and analysis. This could greatly improve the chances of any digital evidence, whether it is an SMS, WhatsApp message, photo or missed call, admissibility in a legal court.

SEAware Training Material Development

The SEAware training material is in a form of a presentation slide set. It is enhanced with inspiring video clips and pictures. It is based on the resulted curriculum presented above. During the training the users can be divided into various groups of four users per group for discussions throughout the training and monitoring. The training covered smartphone background information, the user collection and preservation methods of smartphone data, as well as user safety measure.

SEAware Questionnaire Development

The SEAware questionnaire was also formulated using both the developed SEAware curriculum and training material. The two were used as the guide on the questions to ask that can assess the user's understanding before and after the training. The SEAware questionnaire is divided into three sections, that is, basic demographic information, smartphone evidence collection, preservation and safety measures, and scenarios section. These are described in details below.

a) Questionnaire Part 1: Basic Demographic Information

A short demographic section was included in order to test the authenticity of the user's answers before and after the SEAware training section. These questions mainly test users' use, experience and knowledge of their devices as well as their awareness level on how they use it and if they do think of the purpose of using their smartphone. Various types of questions are used in this section; such as:

- open-ended questions,
- ranking questions, where by user asked to the rank the use of smartphones according to their individual deemed significance, and
- Matrix and rating questions, where users' attitude towards smartphones was tested.

An instruction directing them not to use their devices on the pre-test but on the post-test is included, and permission for this is also obtained in a written consent forms that users can sign prior to completing the questionnaire. Other demographic details might not be easy to ask for unless there is a compelling issue that requires them, ethically. This is mainly to secure privacy of the users.

b) Questionnaire Part 2: Smartphone Evidence - Collection, Preservation and Safety Measures

This subsection and the subsequent one are the most significant sections of the questionnaire as they both focus on smartphone evidence collection, preservation and user safety using various techniques to inspire and instil the digital evidence awareness culture. Most of the questions in this section are balanced between open-ended and closed-ended questions. This structure was chosen in order to give users a platform to make their desired choice and have an additional chance to substantiate it.

Even though it could have saved time for both the users and the researcher to include more of multiple choice questions, it was decided that there might be insufficient data to analyse by the end of the training session. All the questions related to the collection, preservations and user safety were mixed-up evenly, as these are the significant elements of the SEAware training program. These elements were explored further into scenarios questions, as presented on the following subsection. Various types of questions were used in this section; such as:

- open-ended questions,
- multiple choice questions, and
- ranking questions, where user asked to rank the evidence collection methods and to later explain the reason of their first choice.

Users are further presented with a range of circumstances which they could find themselves in; they were also given a chance to use their smartphones for evidence collection and preservation tool. This is to test their response techniques, to compare their level of smartphone evidence awareness and knowledge of dealing with smartphone evidence when they are victims of crime, or witnesses of crime.

c) Questionnaire Part 3: Scenarios

As mentioned above, various types of questions are used in this section; such as

- open-ended questions,
- multiple choice questions, and
- close-ended questions have only two answers, such as "Yes" and "No". These were kept to a minimum as they are too restrictive in terms of choices. To counter this disadvantage, these questions were minimized to only two, with follow up question prompting the user to substantiate their choice (*Wilsdon & Slay, 2006.*).

The questionnaire was structured in such a way that easy questions were at the beginning of the questionnaire and other questions were placed at the end of the questionnaire. This is viewed by SurveyMonkey (2008) as one way of boasting the users' confidence while encouraging them to finish their questionnaire *(SurveyMonkey, 2008)*. Since the SEAware training has an element of awareness, the following section presents the interaction of the SEAware training program with the existing security awareness processes.

THE SEAWARE PROGRAM AND SECURITY AWARENESS PROCESSES

The SEAware components form the basic designs of the SEAware targeted to smartphone users. However, it is useful to firstly define the context of SEAware with respect to how it interacts with other awareness processes. According to National Institute of Standards and Technology (2004) any security awareness program is consists of three phases, that is, preparation, application (or implementation), evaluation (or review) phases *(National Institute of Standards and Technology (NIST), 2004)*. These awareness processes show properties of SEAware training program assist to define context and boundaries within which SEAware training program operate in the awareness environment.

Preparation Phase: SEAware Program Development

This is the beginning process, which is constituted three cyclic-phases:

- Plan phases: is about designing the SEAware training program, assessing its content and selecting appropriate controls;
- Implementing phases: involves Application or implementing and operating the controls and
- Review phases: review and evaluate the performance (efficiency and effectiveness) of the SEAware program, including making changes where necessary to bring the SEAware program to it best performance (*Allgeier, 2000 & Williams, 2007.*). This phase focused on the research that needed to be conducted on each sub-phase. This is shown in Figure 2.

Figure 2 illustrates three different sub-phases that were conducted under the preparation phase as well as the success factors associated with each sub-phase. During planning sub-phase, the focus is on the inputs of the team member, management, etc. These were used to formulate the SEAware program strategy as an output. During the implementation sub-phase, the focus is mainly on the techniques and methods to be used during the roll out of the SEAware program, it also has success factors. The resulted output expected includes presentation material, pre-and post-tests (Wright, 2007 & von Solms, 2006). The methods used were strategized to questionnaires, presentations, discussion topics and evaluation of the program. The last sub-phase of the preparation is the review sub-phase which is consists of the assessment of the both the plan and the implementation of the preparation phase. The expected results include lessons learnt as well as the analysed results of the other two sub-phases.

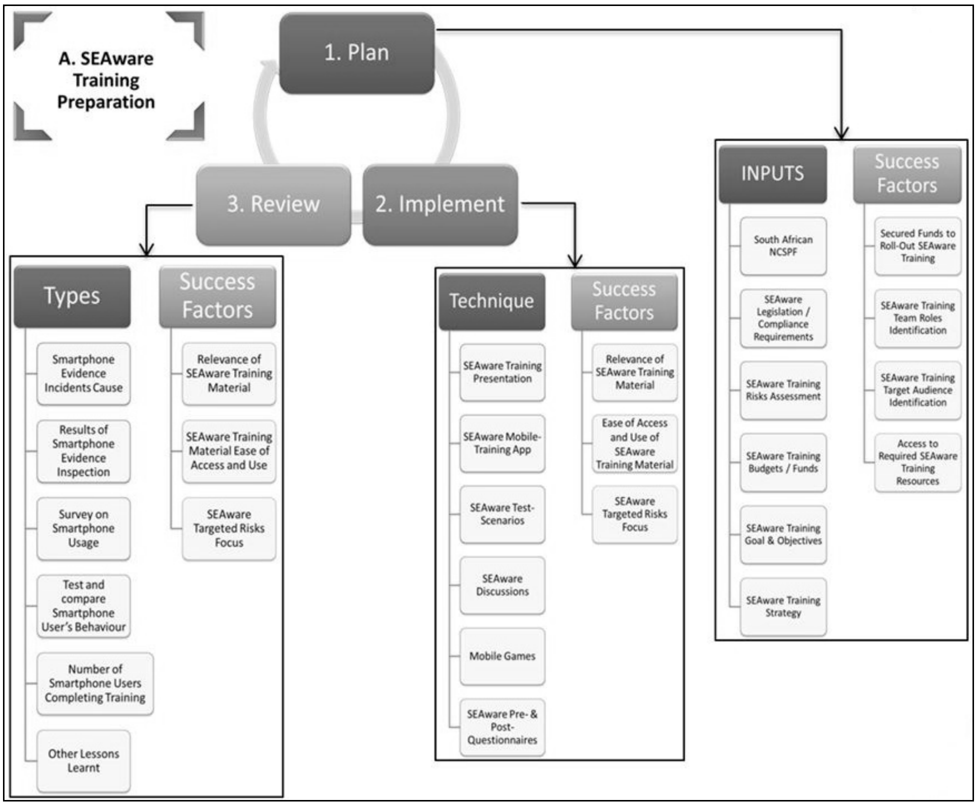
A. SEAware Training Preparation
1. Plan
2. Implement
3. Review
INPUTS
South African NCSPF
SEAware Legislation / Compliance Requirements
SEAware Training Risks Assessment
SEAware Training Budgets / Funds
SEAware Training Goal & Objectives
SEAware Training Strategy
Success Factors
Secured Funds to Roll-Out SEAware Training
SEAware Training Team Roles Identification
SEAware Training Target Audience Identification
Access to Required SEAware Training Resources
Technique
SEAware Training Presentation
SEAware Mobile-Training App
SEAware Test-Scenarios
SEAware Discussions
Mobile Games
SEAware Pre- & Post-Questionnaires
Success Factors
Relevance of SEAware Training Material
Ease of Access and Use of SEAware Training Material
SEAware Targeted Risks Focus
Types
Smartphone Evidence Incidents Cause
Results of Smartphone Evidence Inspection
Survey on Smartphone Usage
Test and compare Smartphone User's Behaviour
Number of Smartphone Users Completing Training
Other Lessons Learnt
Success Factors
Relevance of SEAware Training Material
SEAware Training Material Ease of Access and Use
SEAware Targeted Risks Focus

Figure 2. SEAware Preparation Phase

The preparation phase results to the well planned assessed, reviewed and revised strategy plan (in Table 2 below), ready for actual program. These are used during the application phase in presented next.

Table 2. 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 - To train a group of smartphone users on effective ways of safely collecting and preserving admissible data - To present analyzed 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 - Role of evidence - Smartphone evidence collection - Smartphone evidence preservation - User safety measures
Target Audience	Smartphone users
Delivery Methods	Presentation and group discussion
Evaluation	Pre- and Post- Questionnaire

Application Phase: SEAware Training

This phase, shown in Figure 3 includes the SEAware implementation of the strategy plan in Table 2. This is the roll-out of the SEAware program. It includes the sequence of:

SEAware pre-test,
SEAware training,
SEAware discussion groups' session and
SEAware post-test

The main output collected from the application phase includes the filled pre- and post-test. Other output may include discussion notes and filled SEAware evaluation forms. These are all significant for the next phase, Evaluation phase.

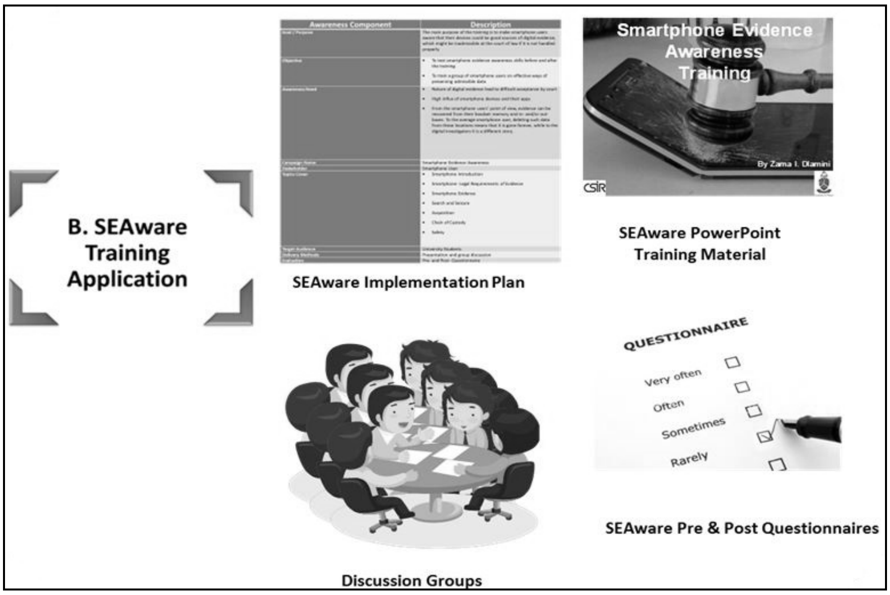
B. SEAware Training Application
SEAware Implementation Plan
Smartphone Evidence Awareness Training
By Zama I. Dlamini
CSIR
SEAware PowerPoint Training Material
QUESTIONNAIRE
Very often □
Often □
Sometimes ☑
Rarely □
SEAware Pre & Post Questionnaires
Discussion Groups

Figure 3. SEAware Application Phase

Evaluation Phase: SEAware Training Evaluation

This is the last phase. It uses the output received from implementation (or application) phase from the above section and presented in Figure 4.

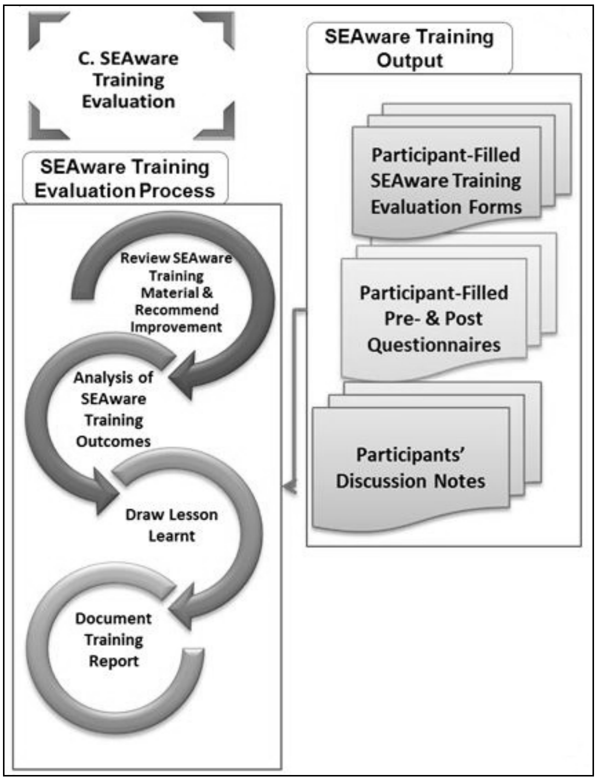
C. SEAware Training Evaluation
SEAware Training Output
Participant-Filled SEAware Training Evaluation Forms
Participant-Filled Pre- & Post Questionnaires
Participants' Discussion Notes
SEAware Training Evaluation Process
Review SEAware Training Material & Recommend Improvement
Analysis of SEAware Training Outcomes
Draw Lesson Learnt
Document Training Report

Figure 4. SEAware Application Phase

During this phase, all the filled forms, pre- and post- questionnaires as well as the group discussion notes are analysed, evaluated, recommendations are prepared and the training report is documented. The awareness process is cyclic, meaning it does not end on the third phase *(Peltier, 2005 & Wright, Burleson, 2007).* The output of the third phase, such as lessons learnt, should be used as input to the first phase in order to update the training documents, methods used as well as the implementation plan; in order to improve the SEAware training program this can be applied.

BENEFITS OF THE SEAWARE TRAINING PROGRAM

The SEAware framework has been developed to make users aware of the integrity of evidence that can be deliberate collected by an average user, resulting to it being compromised by way of incorrect collection, storage or handling requirements. The effect of this program is evaluated through the development and experimental implementation of the SEAware training material (in Table 2) to a group of smartphone users. This paper presented the design of the SEAware training program 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.

The above learning components of the SEAware training framework were used to develop the curriculum, training material and the questionnaire to be used during the training. This study further improves evidence preservation on the cases where smartphones devices are used as source of evidence to confirm users' side of the story 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 *(Zwick, 200 &, Zantyko, 2007*). This simplifies the investigation process and improves admissibility of evidence at court when smartphone users are aware of the capabilities of their devices. The proposed program, SEAware training program, 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.

CONCLUSION

For many years the legal system relied on eyewitnesses, which with time evolved to digital. The capability of electronic devices is continuously improving, but it is still a challenge to keep track of all information that is flowing around, as it is here today and not there tomorrow. Even though the younger generation is relying more on the digital world, there is still a need for their contribution on operating and maintaining these developments. It is still a challenge to do so as the development of technology-based devices and their enhancement is faster than the rate which one could grab. The developed SEAware training program in this paper is designed specifically to train smartphone users on the significance of smartphone data, its safe collection methods and its preservation techniques. The SEAware training program covers smartphone background information, the role of evidence in general, the smartphone evidence collection, smartphone evidence preservation as well as the best practices. This program focuses on smartphone evidence at the user level and does not cover other Digital Forensic investigation processes such as seizure, examination, analysis and presentation. It is consists of SEAware curriculum, training material questionnaire. These are all monitored and maintained by following the awareness process presented as well, which is consists of three phases: preparation, application and evaluation phases. Future work includes the SEAware experiment which will be consists of training, data collection and analysis of a group of smartphone users. This will be used to determine parts of the SEAware training program that are understood and will benefit users in future and which parts need further development. This experiment, where users are trained and the impact of various facets of the program measured will be designed to proceed as follows: selection and recruitment of volunteers; administration of a pre-training questionnaire to determine user behaviour and existing knowledge; training of volunteers through seminars according to the SEAware training framework and program; and administration of a post-training questionnaire to determine knowledge gained and the possible impact of such knowledge on user behaviour.

REFERENCES

Allgeier, M. (2000). Digital media forensics [WWW Document]. Secur. Online. URL http://www.symantec.com/connect/articles/digital-media-forensics (accessed 12.20.13).

Arthur, K., Olivier, M., Venter, H. (2007). Applying the Biba Integrity Model to Evidence Management, in: Advances in Digital Forensics III. Springer, pp. 317–327.

Association of Chief Police Officers (ACPO). (2008). Good Practice Guide for Computer-Based Electronic Evidence.

Ayers, R. (2007). Cell phone forensic tools: an overview and analysis update, 1st ed. CreateSpace Independent Publishing Platform, USA.

Breeuwsma, M., De Jongh, M., Klaver, C., Van Der Knijff, R., Roeloffs, M. (2007). Forensic data recovery from flash memory. Small Scale Digit. Device Forensics J. 1, 1–17.

Brockett, P.L., Golden, L.L., Song, A. (2012). Managing risk in mobile commerce. Int. J. Electron. Bus. 10, 167–184.

Brodie. (2008). The importance of Security Awareness Training.

BusinessTech. (2014). South Africa's most popular smartphone brands.

Carrier, B., Spafford, E.H. (2003). Getting physical with the digital investigation process. Int. J. Digit. Evid. 2, 1–20.

Carrier, B.D. (2006). Risks of live digital forensic analysis. Commun. ACM 49, 56–61.

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

Casey, E., Ferraro, M., Nguyen, L. (2009). Investigation Delayed Is Justice Denied: Proposals for Expediting Forensic Examinations of Digital Evidence*. J. Forensic Sci. 54, 1353–1364.

Duncan, A. (2014). African mobile subscriptions set for huge spike | Fin24 [WWW Document]. Fin24tech. URL http://www.fin24.com/tech/mobile/african-mobile-subscriptions-set-for-huge-spike-20141106 (accessed 11.18.14).

eMarketer. (2014). Smartphone Users Worldwide Will Total 1.75 Billion in 2014.

Ferguson, C.J. (2013). The CSI Effect, in: Adolescents, Crime, and the Media. Springer, pp. 69–80.

Hosmer, C., Jeffcoat, C., Davis, M., McGibbon, T. (2011). Use of Mobile Technology for Information Collection and Dissemination (Technical No. 518055), A DACS Technology Assessment Report. DACS DAN, Conway and Utica.

Mamello, M. (2014). Vodacom launches SA-targeted tablet [WWW Document]. Fin24tech. URL http://www.fin24.com/tech/companies/vodacom-launches-low-cost-tablet-20141014

National Institute of Standards and Technology (NIST). (2004). Digital Data Acquisition Tool Specification.

Nielsenwire. (2012). In U.S. Smartphone Market, Android is Top Operating System. Apple is Top Manufacturer.

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).

PC Magazine. (2011). Smartphone Definition from PC Magazine Encyclopedia. PC Mag.

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

South African Qualification Authority. (2001). Criteria and Guidelines for Assessment of NQF Registered Unit standards and Qualifications.

Stevens, D.J. (2011). Media and criminal justice: The CSI effect. Jones & Bartlett Publishers.

SurveyMonkey. (2008). Smart Survey Design.

Vuyo Mkize of IOL News. (2012). Deleted videos “compromise Jub Jub evidence” - Crime & Courts [WWW Document]. URL http://www.iol.co.za/news/crime-courts/deleted-videos-compromise-jub-jub-evidence-1.1311957#.VLgU-XvSs90 (accessed 1.15.15).

von Solms, S., Louwrens, C., Com, C.R.D., Grobler, T. (2006). A control framework for digital forensics, in: Advances in Digital Forensics II. Springer, pp. 343–355.

Vuyo Mkize of IOL News. (2012). Deleted videos “compromise Jub Jub evidence” - Crime & Courts [WWW Document]. URL http://www.iol.co.za/news/crime-courts/deleted-videos-compromise-jub-jub-evidence-1.1311957#.VLgU-XvSs90 (accessed 1.15.15).

Williams, C. (2007). Research Methods. Journal of Business & Economic Research 5, 8.

Wilsdon, T., Slay, J. (2006). Forensic computing tool testing utilizing black box techniques. Presented at the Proceedings of the 4th Australian Digital Forensics Conference.

Wright, P. (2007). Oracle Forensics in a Nutshell [WWW Document]. URL http://www.oracleforensics.com/wordpress/wp-content/uploads/2007/03/OracleForensicsInANutshell.pdf (accessed 7.16.14).

Wright, P., Burleson, Do. (2007). Oracle Forensics: Oracle Security Best Practices, 1st ed, Oracle In-Focus series. Rampant Techpress, Canada.

Zantyko, K. (2007). Commentary: Defining Digital Forensics [WWW Document]. Forensic Mag. URL http://www.forensicmag.com/articles/2007/01/commentary-defining-digital-forensics (accessed 12.20.13).

Zwick, C. (2005). Designing for small screens: mobile phones, smart phones, PDAs, pocket PCs, navigation systems, MP3 players, game consoles, 1st ed. Ava Publishing.